Panduan Referensi

AWS Kebijakan Terkelola

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Kebijakan Terkelola: Panduan Referensi

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu kebijakan yang AWS dikelola? 1
Memahami halaman referensi kebijakan 1
Kebijakan terkelola yang tidak digunakan lagi AWS 2
AWS kebijakan terkelola 3
AccessAnalyzerServiceRolePolicy 57
Menggunakan kebijakan ini 57
Detail kebijakan 57
Versi kebijakan 57
Dokumen kebijakan JSON 58
Pelajari selengkapnya 60
AccountAccessManagerServiceRolePolicy 60
Menggunakan kebijakan ini 61
Detail kebijakan 61
Versi kebijakan 61
Dokumen kebijakan JSON 61
Pelajari selengkapnya 62
AccountManagementFromVercel 62
Menggunakan kebijakan ini 62
Detail kebijakan 62
Versi kebijakan 62
Dokumen kebijakan JSON 63
Pelajari selengkapnya 64
AdministratorAccess 64
Menggunakan kebijakan ini 65
Detail kebijakan 65
Versi kebijakan 65
Dokumen kebijakan JSON 65
Pelajari selengkapnya 65
AdministratorAccess-Amplify 66
Menggunakan kebijakan ini 66
Detail kebijakan 66
Versi kebijakan 66
Dokumen kebijakan JSON 66
Pelajari selengkapnya 77

AdministratorAccess-AWSElasticBeanstalk 77
Menggunakan kebijakan ini 77
Detail kebijakan 77
Versi kebijakan 77
Dokumen kebijakan JSON 78
Pelajari selengkapnya 86
AgentRegistryFullAccess 86
Menggunakan kebijakan ini 86
Detail kebijakan 86
Versi kebijakan 87
Dokumen kebijakan JSON 87
Pelajari selengkapnya 90
AgentRegistryReadOnlyAccess 91
Menggunakan kebijakan ini 91
Detail kebijakan 91
Versi kebijakan 91
Dokumen kebijakan JSON 91
Pelajari selengkapnya 92
AIDevOpsAgentAccessPolicy 92
Menggunakan kebijakan ini 92
Detail kebijakan 92
Versi kebijakan 92
Dokumen kebijakan JSON 93
Pelajari selengkapnya 115
AIDevOpsAgentActionsPolicy 116
Menggunakan kebijakan ini 116
Detail kebijakan 116
Versi kebijakan 116
Dokumen kebijakan JSON 116
Pelajari selengkapnya 117
AIDevOpsAgentFullAccess 117
Menggunakan kebijakan ini 118
Detail kebijakan 118
Versi kebijakan 118
Dokumen kebijakan JSON 118
Pelajari selengkapnya 120

AIDevOpsAgentReadOnlyAccess 121
Menggunakan kebijakan ini 121
Detail kebijakan 121
Versi kebijakan 121
Dokumen kebijakan JSON 121
Pelajari selengkapnya 122
AIDevOpsChannelAccessPolicy 122
Menggunakan kebijakan ini 122
Detail kebijakan 122
Versi kebijakan 122
Dokumen kebijakan JSON 123
Pelajari selengkapnya 123
AIDevOpsConstellationAccessPolicy 123
Menggunakan kebijakan ini 124
Detail kebijakan 124
Versi kebijakan 124
Dokumen kebijakan JSON 124
Pelajari selengkapnya 125
AIDevOpsOperatorAppAccessPolicy 125
Menggunakan kebijakan ini 125
Detail kebijakan 125
Versi kebijakan 125
Dokumen kebijakan JSON 126
Pelajari selengkapnya 129
AIDevOpsReleaseManagementVPCPolicy 129
Menggunakan kebijakan ini 129
Detail kebijakan 129
Versi kebijakan 129
Dokumen kebijakan JSON 130
Pelajari selengkapnya 132
AIOpsAssistantIncidentReportPolicy 133
Menggunakan kebijakan ini 133
Detail kebijakan 133
Versi kebijakan 133
Dokumen kebijakan JSON 133
Pelajari selengkapnya 134

AIOpsAssistantPolicy 134
Menggunakan kebijakan ini 135
Detail kebijakan 135
Versi kebijakan 135
Dokumen kebijakan JSON 135
Pelajari selengkapnya 156
AIOpsConsoleAdminPolicy 156
Menggunakan kebijakan ini 156
Detail kebijakan 156
Versi kebijakan 156
Dokumen kebijakan JSON 157
Pelajari selengkapnya 163
AIOpsOperatorAccess 163
Menggunakan kebijakan ini 163
Detail kebijakan 163
Versi kebijakan 163
Dokumen kebijakan JSON 164
Pelajari selengkapnya 166
AIOpsReadOnlyAccess 167
Menggunakan kebijakan ini 167
Detail kebijakan 167
Versi kebijakan 167
Dokumen kebijakan JSON 167
Pelajari selengkapnya 168
AlexaForBusinessDeviceSetup 168
Menggunakan kebijakan ini 168
Detail kebijakan 168
Versi kebijakan 169
Dokumen kebijakan JSON 169
Pelajari selengkapnya 169
AlexaForBusinessFullAccess 170
Menggunakan kebijakan ini 170
Detail kebijakan 170
Versi kebijakan 170
Dokumen kebijakan JSON 170
Pelajari selengkapnya 172

AlexaForBusinessGatewayExecution 172
Menggunakan kebijakan ini 172
Detail kebijakan 172
Versi kebijakan 172
Dokumen kebijakan JSON 173
Pelajari selengkapnya 173
AlexaForBusinessLifesizeDelegatedAccessPolicy 174
Menggunakan kebijakan ini 174
Detail kebijakan 174
Versi kebijakan 174
Dokumen kebijakan JSON 174
Pelajari selengkapnya 177
AlexaForBusinessNetworkProfileServicePolicy 177
Menggunakan kebijakan ini 177
Detail kebijakan 177
Versi kebijakan 177
Dokumen kebijakan JSON 178
Pelajari selengkapnya 178
AlexaForBusinessPolyDelegatedAccessPolicy 178
Menggunakan kebijakan ini 179
Detail kebijakan 179
Versi kebijakan 179
Dokumen kebijakan JSON 179
Pelajari selengkapnya 181
AlexaForBusinessReadOnlyAccess 181
Menggunakan kebijakan ini 181
Detail kebijakan 181
Versi kebijakan 182
Dokumen kebijakan JSON 182
Pelajari selengkapnya 182
AmazonAPIGatewayAdministrator 182
Menggunakan kebijakan ini 183
Detail kebijakan 183
Versi kebijakan 183
Dokumen kebijakan JSON 183
Pelajari selengkapnya 183

AmazonAPIGatewayInvokeFullAccess 184
Menggunakan kebijakan ini 184
Detail kebijakan 184
Versi kebijakan 184
Dokumen kebijakan JSON 184
Pelajari selengkapnya 185
AmazonAPIGatewayPushToCloudWatchLogs 185
Menggunakan kebijakan ini 185
Detail kebijakan 185
Versi kebijakan 185
Dokumen kebijakan JSON 186
Pelajari selengkapnya 186
AmazonAppFlowFullAccess 186
Menggunakan kebijakan ini 187
Detail kebijakan 187
Versi kebijakan 187
Dokumen kebijakan JSON 187
Pelajari selengkapnya 190
AmazonAppFlowReadOnlyAccess 190
Menggunakan kebijakan ini 190
Detail kebijakan 190
Versi kebijakan 190
Dokumen kebijakan JSON 191
Pelajari selengkapnya 191
AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy 191
Menggunakan kebijakan ini 192
Detail kebijakan 192
Versi kebijakan 192
Dokumen kebijakan JSON 192
Pelajari selengkapnya 193
AmazonAppStreamFullAccess 194
Menggunakan kebijakan ini 194
Detail kebijakan 194
Versi kebijakan 194
Dokumen kebijakan JSON 194
Pelajari selengkapnya 196

AmazonAppStreamPCAAccess 196
Menggunakan kebijakan ini 196
Detail kebijakan 197
Versi kebijakan 197
Dokumen kebijakan JSON 197
Pelajari selengkapnya 197
AmazonAppStreamReadOnlyAccess 198
Menggunakan kebijakan ini 198
Detail kebijakan 198
Versi kebijakan 198
Dokumen kebijakan JSON 198
Pelajari selengkapnya 199
AmazonAppStreamServiceAccess 199
Menggunakan kebijakan ini 199
Detail kebijakan 199
Versi kebijakan 199
Dokumen kebijakan JSON 200
Pelajari selengkapnya 201
AmazonAthenaFullAccess 201
Menggunakan kebijakan ini 201
Detail kebijakan 201
Versi kebijakan 201
Dokumen kebijakan JSON 202
Pelajari selengkapnya 205
AmazonAthenaServiceRolePolicy 205
Menggunakan kebijakan ini 205
Detail kebijakan 206
Versi kebijakan 206
Dokumen kebijakan JSON 206
Pelajari selengkapnya 207
AmazonAugmentedAIFullAccess 207
Menggunakan kebijakan ini 207
Detail kebijakan 207
Versi kebijakan 207
Dokumen kebijakan JSON 207
Pelajari selengkapnya 208

AmazonAugmentedAIHumanLoopFullAccess 209
Menggunakan kebijakan ini 209
Detail kebijakan 209
Versi kebijakan 209
Dokumen kebijakan JSON 209
Pelajari selengkapnya 210
AmazonAugmentedAIIntegratedAPIAccess 210
Menggunakan kebijakan ini 210
Detail kebijakan 210
Versi kebijakan 210
Dokumen kebijakan JSON 211
Pelajari selengkapnya 212
AmazonAuroraDSQLConsoleFullAccess 212
Menggunakan kebijakan ini 212
Detail kebijakan 212
Versi kebijakan 213
Dokumen kebijakan JSON 213
Pelajari selengkapnya 215
AmazonAuroraDSQLFullAccess 215
Menggunakan kebijakan ini 216
Detail kebijakan 216
Versi kebijakan 216
Dokumen kebijakan JSON 216
Pelajari selengkapnya 219
AmazonAuroraDSQLReadOnlyAccess 219
Menggunakan kebijakan ini 219
Detail kebijakan 219
Versi kebijakan 219
Dokumen kebijakan JSON 220
Pelajari selengkapnya 220
AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy 220
Menggunakan kebijakan ini 221
Detail kebijakan 221
Versi kebijakan 221
Dokumen kebijakan JSON 221
Pelajari selengkapnya 222

AmazonBedrockExternalWebSearchFullAccess 222
Menggunakan kebijakan ini 223
Detail kebijakan 223
Versi kebijakan 223
Dokumen kebijakan JSON 223
Pelajari selengkapnya 224
AmazonBedrockExternalWebSearchReadOnly 224
Menggunakan kebijakan ini 224
Detail kebijakan 224
Versi kebijakan 224
Dokumen kebijakan JSON 224
Pelajari selengkapnya 225
AmazonBedrockFullAccess 225
Menggunakan kebijakan ini 225
Detail kebijakan 225
Versi kebijakan 226
Dokumen kebijakan JSON 226
Pelajari selengkapnya 231
AmazonBedrockLimitedAccess 231
Menggunakan kebijakan ini 231
Detail kebijakan 232
Versi kebijakan 232
Dokumen kebijakan JSON 232
Pelajari selengkapnya 235
AmazonBedrockMantleFullAccess 235
Menggunakan kebijakan ini 235
Detail kebijakan 235
Versi kebijakan 235
Dokumen kebijakan JSON 236
Pelajari selengkapnya 236
AmazonBedrockMantleInferenceAccess 237
Menggunakan kebijakan ini 237
Detail kebijakan 237
Versi kebijakan 237
Dokumen kebijakan JSON 237
Pelajari selengkapnya 239

AmazonBedrockMantleReadOnly 239
Menggunakan kebijakan ini 239
Detail kebijakan 239
Versi kebijakan 239
Dokumen kebijakan JSON 239
Pelajari selengkapnya 240
AmazonBedrockMarketplaceAccess 240
Menggunakan kebijakan ini 240
Detail kebijakan 241
Versi kebijakan 241
Dokumen kebijakan JSON 241
Pelajari selengkapnya 245
AmazonBedrockReadOnly 245
Menggunakan kebijakan ini 246
Detail kebijakan 246
Versi kebijakan 246
Dokumen kebijakan JSON 246
Pelajari selengkapnya 247
AmazonBedrockStudioPermissionsBoundary 248
Menggunakan kebijakan ini 248
Detail kebijakan 248
Versi kebijakan 248
Dokumen kebijakan JSON 248
Pelajari selengkapnya 252
AmazonBedrockWebSearchFullAccess 253
Menggunakan kebijakan ini 253
Detail kebijakan 253
Versi kebijakan 253
Dokumen kebijakan JSON 253
Pelajari selengkapnya 254
AmazonBedrockWebSearchReadOnly 254
Menggunakan kebijakan ini 254
Detail kebijakan 254
Versi kebijakan 254
Dokumen kebijakan JSON 255
Pelajari selengkapnya 255

AmazonBioDiscoveryFullAccess 255
Menggunakan kebijakan ini 255
Detail kebijakan 255
Versi kebijakan 256
Dokumen kebijakan JSON 256
Pelajari selengkapnya 258
AmazonBioDiscoveryInAppFullAccess 259
Menggunakan kebijakan ini 259
Detail kebijakan 259
Versi kebijakan 259
Dokumen kebijakan JSON 259
Pelajari selengkapnya 261
AmazonBraketFullAccess 261
Menggunakan kebijakan ini 261
Detail kebijakan 261
Versi kebijakan 262
Dokumen kebijakan JSON 262
Pelajari selengkapnya 267
AmazonBraketJobsExecutionPolicy 267
Menggunakan kebijakan ini 267
Detail kebijakan 267
Versi kebijakan 267
Dokumen kebijakan JSON 267
Pelajari selengkapnya 270
AmazonBraketServiceRolePolicy 271
Menggunakan kebijakan ini 271
Detail kebijakan 271
Versi kebijakan 271
Dokumen kebijakan JSON 271
Pelajari selengkapnya 273
AmazonChimeFullAccess 273
Menggunakan kebijakan ini 273
Detail kebijakan 273
Versi kebijakan 273
Dokumen kebijakan JSON 273
Pelajari selengkapnya 275

AmazonChimeReadOnly 276
Menggunakan kebijakan ini 276
Detail kebijakan 276
Versi kebijakan 276
Dokumen kebijakan JSON 276
Pelajari selengkapnya 277
AmazonChimeSDK 277
Menggunakan kebijakan ini 277
Detail kebijakan 277
Versi kebijakan 277
Dokumen kebijakan JSON 278
Pelajari selengkapnya 279
AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy 279
Menggunakan kebijakan ini 279
Detail kebijakan 279
Versi kebijakan 279
Dokumen kebijakan JSON 280
Pelajari selengkapnya 281
AmazonChimeSDKMessagingServiceRolePolicy 281
Menggunakan kebijakan ini 281
Detail kebijakan 281
Versi kebijakan 282
Dokumen kebijakan JSON 282
Pelajari selengkapnya 283
AmazonChimeServiceRolePolicy 283
Menggunakan kebijakan ini 283
Detail kebijakan 283
Versi kebijakan 283
Dokumen kebijakan JSON 283
Pelajari selengkapnya 284
AmazonChimeTranscriptionServiceLinkedRolePolicy 284
Menggunakan kebijakan ini 284
Detail kebijakan 284
Versi kebijakan 285
Dokumen kebijakan JSON 285
Pelajari selengkapnya 285

AmazonChimeUserManagement 285
Menggunakan kebijakan ini 286
Detail kebijakan 286
Versi kebijakan 286
Dokumen kebijakan JSON 286
Pelajari selengkapnya 287
AmazonChimeVoiceConnectorServiceLinkedRolePolicy 287
Menggunakan kebijakan ini 288
Detail kebijakan 288
Versi kebijakan 288
Dokumen kebijakan JSON 288
Pelajari selengkapnya 290
AmazonCloudDirectoryFullAccess 290
Menggunakan kebijakan ini 290
Detail kebijakan 290
Versi kebijakan 291
Dokumen kebijakan JSON 291
Pelajari selengkapnya 291
AmazonCloudDirectoryReadOnlyAccess 291
Menggunakan kebijakan ini 292
Detail kebijakan 292
Versi kebijakan 292
Dokumen kebijakan JSON 292
Pelajari selengkapnya 293
AmazonCloudWatchEvidentlyFullAccess 293
Menggunakan kebijakan ini 293
Detail kebijakan 293
Versi kebijakan 293
Dokumen kebijakan JSON 293
Pelajari selengkapnya 296
AmazonCloudWatchEvidentlyReadOnlyAccess 296
Menggunakan kebijakan ini 296
Detail kebijakan 296
Versi kebijakan 297
Dokumen kebijakan JSON 297
Pelajari selengkapnya 297

AmazonCloudWatchEvidentlyServiceRolePolicy 298
Menggunakan kebijakan ini 298
Detail kebijakan 298
Versi kebijakan 298
Dokumen kebijakan JSON 298
Pelajari selengkapnya 300
AmazonCloudWatchRUMFullAccess 300
Menggunakan kebijakan ini 300
Detail kebijakan 300
Versi kebijakan 300
Dokumen kebijakan JSON 301
Pelajari selengkapnya 303
AmazonCloudWatchRUMReadOnlyAccess 303
Menggunakan kebijakan ini 303
Detail kebijakan 303
Versi kebijakan 304
Dokumen kebijakan JSON 304
Pelajari selengkapnya 305
AmazonCloudWatchRUMServiceRolePolicy 305
Menggunakan kebijakan ini 306
Detail kebijakan 306
Versi kebijakan 306
Dokumen kebijakan JSON 306
Pelajari selengkapnya 307
AmazonCodeCatalystFullAccess 307
Menggunakan kebijakan ini 307
Detail kebijakan 307
Versi kebijakan 307
Dokumen kebijakan JSON 308
Pelajari selengkapnya 308
AmazonCodeCatalystReadOnlyAccess 309
Menggunakan kebijakan ini 309
Detail kebijakan 309
Versi kebijakan 309
Dokumen kebijakan JSON 309
Pelajari selengkapnya 310

AmazonCodeCatalystSupportAccess 310
Menggunakan kebijakan ini 310
Detail kebijakan 310
Versi kebijakan 310
Dokumen kebijakan JSON 311
Pelajari selengkapnya 311
AmazonCodeGuruProfilerAgentAccess 312
Menggunakan kebijakan ini 312
Detail kebijakan 312
Versi kebijakan 312
Dokumen kebijakan JSON 312
Pelajari selengkapnya 313
AmazonCodeGuruProfilerFullAccess 313
Menggunakan kebijakan ini 313
Detail kebijakan 313
Versi kebijakan 313
Dokumen kebijakan JSON 314
Pelajari selengkapnya 314
AmazonCodeGuruProfilerReadOnlyAccess 315
Menggunakan kebijakan ini 315
Detail kebijakan 315
Versi kebijakan 315
Dokumen kebijakan JSON 315
Pelajari selengkapnya 316
AmazonCodeGuruReviewerFullAccess 316
Menggunakan kebijakan ini 316
Detail kebijakan 316
Versi kebijakan 316
Dokumen kebijakan JSON 317
Pelajari selengkapnya 319
AmazonCodeGuruReviewerReadOnlyAccess 319
Menggunakan kebijakan ini 320
Detail kebijakan 320
Versi kebijakan 320
Dokumen kebijakan JSON 320
Pelajari selengkapnya 321

AmazonCodeGuruReviewerServiceRolePolicy 321
Menggunakan kebijakan ini 321
Detail kebijakan 321
Versi kebijakan 321
Dokumen kebijakan JSON 322
Pelajari selengkapnya 324
AmazonCodeGuruSecurityFullAccess 324
Menggunakan kebijakan ini 324
Detail kebijakan 324
Versi kebijakan 324
Dokumen kebijakan JSON 324
Pelajari selengkapnya 325
AmazonCodeGuruSecurityScanAccess 325
Menggunakan kebijakan ini 325
Detail kebijakan 325
Versi kebijakan 325
Dokumen kebijakan JSON 326
Pelajari selengkapnya 326
AmazonCognitoDeveloperAuthenticatedIdentities 326
Menggunakan kebijakan ini 327
Detail kebijakan 327
Versi kebijakan 327
Dokumen kebijakan JSON 327
Pelajari selengkapnya 328
AmazonCognitoIdpEmailServiceRolePolicy 328
Menggunakan kebijakan ini 328
Detail kebijakan 328
Versi kebijakan 328
Dokumen kebijakan JSON 329
Pelajari selengkapnya 329
AmazonCognitoIdpServiceRolePolicy 329
Menggunakan kebijakan ini 329
Detail kebijakan 330
Versi kebijakan 330
Dokumen kebijakan JSON 330
Pelajari selengkapnya 330

AmazonCognitoPowerUser 331
Menggunakan kebijakan ini 331
Detail kebijakan 331
Versi kebijakan 331
Dokumen kebijakan JSON 331
Pelajari selengkapnya 333
AmazonCognitoReadOnly 333
Menggunakan kebijakan ini 333
Detail kebijakan 333
Versi kebijakan 333
Dokumen kebijakan JSON 333
Pelajari selengkapnya 334
AmazonCognitoUnAuthedIdentitiesSessionPolicy 334
Menggunakan kebijakan ini 335
Detail kebijakan 335
Versi kebijakan 335
Dokumen kebijakan JSON 335
Pelajari selengkapnya 336
AmazonCognitoUnauthenticatedIdentities 336
Menggunakan kebijakan ini 337
Detail kebijakan 337
Versi kebijakan 337
Dokumen kebijakan JSON 337
Pelajari selengkapnya 338
AmazonConnect_FullAccess 338
Menggunakan kebijakan ini 338
Detail kebijakan 338
Versi kebijakan 338
Dokumen kebijakan JSON 339
Pelajari selengkapnya 341
AmazonConnectCampaignsServiceLinkedRolePolicy 341
Menggunakan kebijakan ini 342
Detail kebijakan 342
Versi kebijakan 342
Dokumen kebijakan JSON 342
Pelajari selengkapnya 346

AmazonConnectReadOnlyAccess 346
Menggunakan kebijakan ini 346
Detail kebijakan 346
Versi kebijakan 346
Dokumen kebijakan JSON 346
Pelajari selengkapnya 347
AmazonConnectServiceLinkedRolePolicy 347
Menggunakan kebijakan ini 347
Detail kebijakan 347
Versi kebijakan 348
Dokumen kebijakan JSON 348
Pelajari selengkapnya 357
AmazonConnectSynchronizationServiceRolePolicy 357
Menggunakan kebijakan ini 357
Detail kebijakan 357
Versi kebijakan 357
Dokumen kebijakan JSON 357
Pelajari selengkapnya 359
AmazonConnectVoiceIDFullAccess 359
Menggunakan kebijakan ini 360
Detail kebijakan 360
Versi kebijakan 360
Dokumen kebijakan JSON 360
Pelajari selengkapnya 360
AmazonDataZoneBedrockModelConsumptionPolicy 361
Menggunakan kebijakan ini 361
Detail kebijakan 361
Versi kebijakan 361
Dokumen kebijakan JSON 361
Pelajari selengkapnya 364
AmazonDataZoneBedrockModelManagementPolicy 364
Menggunakan kebijakan ini 364
Detail kebijakan 364
Versi kebijakan 364
Dokumen kebijakan JSON 365
Pelajari selengkapnya 366

AmazonDataZoneDomainExecutionRolePolicy 367
Menggunakan kebijakan ini 367
Detail kebijakan 367
Versi kebijakan 367
Dokumen kebijakan JSON 367
Pelajari selengkapnya 371
AmazonDataZoneEnvironmentRolePermissionsBoundary 371
Menggunakan kebijakan ini 371
Detail kebijakan 371
Versi kebijakan 372
Dokumen kebijakan JSON 372
Pelajari selengkapnya 385
AmazonDataZoneFullAccess 385
Menggunakan kebijakan ini 385
Detail kebijakan 385
Versi kebijakan 385
Dokumen kebijakan JSON 386
Pelajari selengkapnya 394
AmazonDataZoneFullUserAccess 395
Menggunakan kebijakan ini 395
Detail kebijakan 395
Versi kebijakan 395
Dokumen kebijakan JSON 395
Pelajari selengkapnya 399
AmazonDataZoneGlueManageAccessRolePolicy 399
Menggunakan kebijakan ini 399
Detail kebijakan 399
Versi kebijakan 400
Dokumen kebijakan JSON 400
Pelajari selengkapnya 407
AmazonDataZonePortalFullAccessPolicy 408
Menggunakan kebijakan ini 408
Detail kebijakan 408
Versi kebijakan 408
Dokumen kebijakan JSON 408
Pelajari selengkapnya 409

AmazonDataZonePreviewConsoleFullAccess 409
Menggunakan kebijakan ini 409
Detail kebijakan 409
Versi kebijakan 409
Dokumen kebijakan JSON 410
Pelajari selengkapnya 411
AmazonDataZoneProjectDeploymentPermissionsBoundary 412
Menggunakan kebijakan ini 412
Detail kebijakan 412
Versi kebijakan 412
Dokumen kebijakan JSON 412
Pelajari selengkapnya 420
AmazonDataZoneProjectRolePermissionsBoundary 421
Menggunakan kebijakan ini 421
Detail kebijakan 421
Versi kebijakan 421
Dokumen kebijakan JSON 421
Pelajari selengkapnya 428
AmazonDataZoneRedshiftGlueProvisioningPolicy 429
Menggunakan kebijakan ini 429
Detail kebijakan 429
Versi kebijakan 429
Dokumen kebijakan JSON 429
Pelajari selengkapnya 437
AmazonDataZoneRedshiftManageAccessRolePolicy 437
Menggunakan kebijakan ini 437
Detail kebijakan 438
Versi kebijakan 438
Dokumen kebijakan JSON 438
Pelajari selengkapnya 441
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 441
Menggunakan kebijakan ini 442
Detail kebijakan 442
Versi kebijakan 442
Dokumen kebijakan JSON 442
Pelajari selengkapnya 470

AmazonDataZoneSageMakerManageAccessRolePolicy 470
Menggunakan kebijakan ini 470
Detail kebijakan 470
Versi kebijakan 470
Dokumen kebijakan JSON 471
Pelajari selengkapnya 475
AmazonDataZoneSageMakerProvisioningRolePolicy 475
Menggunakan kebijakan ini 476
Detail kebijakan 476
Versi kebijakan 476
Dokumen kebijakan JSON 476
Pelajari selengkapnya 481
AmazonDetectiveFullAccess 481
Menggunakan kebijakan ini 481
Detail kebijakan 481
Versi kebijakan 481
Dokumen kebijakan JSON 482
Pelajari selengkapnya 483
AmazonDetectiveInvestigatorAccess 483
Menggunakan kebijakan ini 483
Detail kebijakan 483
Versi kebijakan 483
Dokumen kebijakan JSON 484
Pelajari selengkapnya 485
AmazonDetectiveMemberAccess 485
Menggunakan kebijakan ini 485
Detail kebijakan 486
Versi kebijakan 486
Dokumen kebijakan JSON 486
Pelajari selengkapnya 486
AmazonDetectiveOrganizationsAccess 487
Menggunakan kebijakan ini 487
Detail kebijakan 487
Versi kebijakan 487
Dokumen kebijakan JSON 487
Pelajari selengkapnya 489

AmazonDetectiveServiceLinkedRolePolicy 489
Menggunakan kebijakan ini 489
Detail kebijakan 490
Versi kebijakan 490
Dokumen kebijakan JSON 490
Pelajari selengkapnya 490
AmazonDevOpsGuruConsoleFullAccess 491
Menggunakan kebijakan ini 491
Detail kebijakan 491
Versi kebijakan 491
Dokumen kebijakan JSON 491
Pelajari selengkapnya 494
AmazonDevOpsGuruFullAccess 494
Menggunakan kebijakan ini 494
Detail kebijakan 494
Versi kebijakan 494
Dokumen kebijakan JSON 494
Pelajari selengkapnya 497
AmazonDevOpsGuruOrganizationsAccess 497
Menggunakan kebijakan ini 497
Detail kebijakan 497
Versi kebijakan 497
Dokumen kebijakan JSON 498
Pelajari selengkapnya 499
AmazonDevOpsGuruReadOnlyAccess 499
Menggunakan kebijakan ini 499
Detail kebijakan 499
Versi kebijakan 499
Dokumen kebijakan JSON 500
Pelajari selengkapnya 502
AmazonDevOpsGuruServiceRolePolicy 502
Menggunakan kebijakan ini 502
Detail kebijakan 502
Versi kebijakan 502
Dokumen kebijakan JSON 503
Pelajari selengkapnya 507

AmazonDMSCloudWatchLogsRole 507
Menggunakan kebijakan ini 507
Detail kebijakan 507
Versi kebijakan 507
Dokumen kebijakan JSON 507
Pelajari selengkapnya 509
AmazonDMSRedshiftS3Role 509
Menggunakan kebijakan ini 509
Detail kebijakan 509
Versi kebijakan 510
Dokumen kebijakan JSON 510
Pelajari selengkapnya 510
AmazonDMSVPCManagementRole 511
Menggunakan kebijakan ini 511
Detail kebijakan 511
Versi kebijakan 511
Dokumen kebijakan JSON 511
Pelajari selengkapnya 512
AmazonDocDB-ElasticServiceRolePolicy 512
Menggunakan kebijakan ini 512
Detail kebijakan 512
Versi kebijakan 513
Dokumen kebijakan JSON 513
Pelajari selengkapnya 513
AmazonDocDBConsoleFullAccess 514
Menggunakan kebijakan ini 514
Detail kebijakan 514
Versi kebijakan 514
Dokumen kebijakan JSON 514
Pelajari selengkapnya 519
AmazonDocDBElasticFullAccess 519
Menggunakan kebijakan ini 519
Detail kebijakan 519
Versi kebijakan 519
Dokumen kebijakan JSON 520
Pelajari selengkapnya 523

AmazonDocDBElasticReadOnlyAccess 523
Menggunakan kebijakan ini 523
Detail kebijakan 523
Versi kebijakan 523
Dokumen kebijakan JSON 524
Pelajari selengkapnya 524
AmazonDocDBFullAccess 525
Menggunakan kebijakan ini 525
Detail kebijakan 525
Versi kebijakan 525
Dokumen kebijakan JSON 525
Pelajari selengkapnya 528
AmazonDocDBReadOnlyAccess 528
Menggunakan kebijakan ini 528
Detail kebijakan 528
Versi kebijakan 529
Dokumen kebijakan JSON 529
Pelajari selengkapnya 531
AmazonDRSVPCManagement 531
Menggunakan kebijakan ini 531
Detail kebijakan 531
Versi kebijakan 531
Dokumen kebijakan JSON 531
Pelajari selengkapnya 532
AmazonDynamoDBFullAccess 532
Menggunakan kebijakan ini 532
Detail kebijakan 533
Versi kebijakan 533
Dokumen kebijakan JSON 533
Pelajari selengkapnya 536
AmazonDynamoDBFullAccess_v2 536
Menggunakan kebijakan ini 536
Detail kebijakan 536
Versi kebijakan 536
Dokumen kebijakan JSON 536
Pelajari selengkapnya 540

AmazonDynamoDBFullAccesswithDataPipeline 540
Menggunakan kebijakan ini 540
Detail kebijakan 540
Versi kebijakan 540
Dokumen kebijakan JSON 541
Pelajari selengkapnya 543
AmazonDynamoDBReadOnlyAccess 543
Menggunakan kebijakan ini 543
Detail kebijakan 543
Versi kebijakan 543
Dokumen kebijakan JSON 544
Pelajari selengkapnya 545
AmazonEBSCSIDriverEKSClusterScopedPolicy 545
Menggunakan kebijakan ini 546
Detail kebijakan 546
Versi kebijakan 546
Dokumen kebijakan JSON 546
Pelajari selengkapnya 551
AmazonEBSCSIDriverPolicy 551
Menggunakan kebijakan ini 552
Detail kebijakan 552
Versi kebijakan 552
Dokumen kebijakan JSON 552
Pelajari selengkapnya 557
AmazonEBSCSIDriverPolicyV2 557
Menggunakan kebijakan ini 557
Detail kebijakan 557
Versi kebijakan 557
Dokumen kebijakan JSON 558
Pelajari selengkapnya 562
AmazonEC2ContainerRegistryFullAccess 562
Menggunakan kebijakan ini 563
Detail kebijakan 563
Versi kebijakan 563
Dokumen kebijakan JSON 563
Pelajari selengkapnya 564

AmazonEC2ContainerRegistryPowerUser 564
Menggunakan kebijakan ini 564
Detail kebijakan 564
Versi kebijakan 565
Dokumen kebijakan JSON 565
Pelajari selengkapnya 565
AmazonEC2ContainerRegistryPullOnly 566
Menggunakan kebijakan ini 566
Detail kebijakan 566
Versi kebijakan 566
Dokumen kebijakan JSON 566
Pelajari selengkapnya 567
AmazonEC2ContainerRegistryReadOnly 567
Menggunakan kebijakan ini 567
Detail kebijakan 567
Versi kebijakan 567
Dokumen kebijakan JSON 568
Pelajari selengkapnya 568
AmazonEC2ContainerServiceAutoscaleRole 569
Menggunakan kebijakan ini 569
Detail kebijakan 569
Versi kebijakan 569
Dokumen kebijakan JSON 569
Pelajari selengkapnya 570
AmazonEC2ContainerServiceEventsRole 570
Menggunakan kebijakan ini 570
Detail kebijakan 570
Versi kebijakan 571
Dokumen kebijakan JSON 571
Pelajari selengkapnya 572
AmazonEC2ContainerServiceforEC2Role 572
Menggunakan kebijakan ini 572
Detail kebijakan 572
Versi kebijakan 573
Dokumen kebijakan JSON 573
Pelajari selengkapnya 574

AmazonEC2ContainerServiceRole 574
Menggunakan kebijakan ini 574
Detail kebijakan 574
Versi kebijakan 575
Dokumen kebijakan JSON 575
Pelajari selengkapnya 575
AmazonEC2FullAccess 576
Menggunakan kebijakan ini 576
Detail kebijakan 576
Versi kebijakan 576
Dokumen kebijakan JSON 576
Pelajari selengkapnya 577
AmazonEC2ImageReferencesAccessPolicy 578
Menggunakan kebijakan ini 578
Detail kebijakan 578
Versi kebijakan 578
Dokumen kebijakan JSON 578
Pelajari selengkapnya 579
AmazonEC2ReadOnlyAccess 579
Menggunakan kebijakan ini 579
Detail kebijakan 580
Versi kebijakan 580
Dokumen kebijakan JSON 580
Pelajari selengkapnya 581
AmazonEC2RoleforAWSCodeDeploy 581
Menggunakan kebijakan ini 581
Detail kebijakan 581
Versi kebijakan 582
Dokumen kebijakan JSON 582
Pelajari selengkapnya 582
AmazonEC2RoleforAWSCodeDeployLimited 582
Menggunakan kebijakan ini 583
Detail kebijakan 583
Versi kebijakan 583
Dokumen kebijakan JSON 583
Pelajari selengkapnya 584

AmazonEC2RoleforDataPipelineRole 584
Menggunakan kebijakan ini 584
Detail kebijakan 584
Versi kebijakan 585
Dokumen kebijakan JSON 585
Pelajari selengkapnya 585
AmazonEC2RoleforSSM 586
Menggunakan kebijakan ini 586
Detail kebijakan 586
Versi kebijakan 586
Dokumen kebijakan JSON 586
Pelajari selengkapnya 589
AmazonEC2RolePolicyForLaunchWizard 589
Menggunakan kebijakan ini 589
Detail kebijakan 589
Versi kebijakan 589
Dokumen kebijakan JSON 590
Pelajari selengkapnya 594
AmazonEC2SpotFleetAutoscaleRole 594
Menggunakan kebijakan ini 595
Detail kebijakan 595
Versi kebijakan 595
Dokumen kebijakan JSON 595
Pelajari selengkapnya 596
AmazonEC2SpotFleetTaggingRole 596
Menggunakan kebijakan ini 596
Detail kebijakan 597
Versi kebijakan 597
Dokumen kebijakan JSON 597
Pelajari selengkapnya 598
AmazonECS_FullAccess 599
Menggunakan kebijakan ini 599
Detail kebijakan 599
Versi kebijakan 599
Dokumen kebijakan JSON 599
Pelajari selengkapnya 605

AmazonECSComputeServiceRolePolicy 606
Menggunakan kebijakan ini 606
Detail kebijakan 606
Versi kebijakan 606
Dokumen kebijakan JSON 606
Pelajari selengkapnya 608
AmazonECSInfrastructureRoleforExpressGatewayServices 608
Menggunakan kebijakan ini 608
Detail kebijakan 608
Versi kebijakan 608
Dokumen kebijakan JSON 609
Pelajari selengkapnya 615
AmazonECSInfrastructureRoleForGatewayHostSharedALB 615
Menggunakan kebijakan ini 615
Detail kebijakan 616
Versi kebijakan 616
Dokumen kebijakan JSON 616
Pelajari selengkapnya 621
AmazonECSInfrastructureRolePolicyForLoadBalancers 621
Menggunakan kebijakan ini 622
Detail kebijakan 622
Versi kebijakan 622
Dokumen kebijakan JSON 622
Pelajari selengkapnya 623
AmazonECSInfrastructureRolePolicyForManagedInstances 624
Menggunakan kebijakan ini 624
Detail kebijakan 624
Versi kebijakan 624
Dokumen kebijakan JSON 624
Pelajari selengkapnya 629
AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity 629
Menggunakan kebijakan ini 629
Detail kebijakan 630
Versi kebijakan 630
Dokumen kebijakan JSON 630
Pelajari selengkapnya 632

AmazonECSInfrastructureRolePolicyForVolumes 633
Menggunakan kebijakan ini 633
Detail kebijakan 633
Versi kebijakan 633
Dokumen kebijakan JSON 633
Pelajari selengkapnya 636
AmazonECSInfrastructureRolePolicyForVpcLattice 636
Menggunakan kebijakan ini 636
Detail kebijakan 636
Versi kebijakan 636
Dokumen kebijakan JSON 637
Pelajari selengkapnya 638
AmazonECSInstanceRolePolicyForManagedInstances 638
Menggunakan kebijakan ini 639
Detail kebijakan 639
Versi kebijakan 639
Dokumen kebijakan JSON 639
Pelajari selengkapnya 640
AmazonECSServiceRolePolicy 641
Menggunakan kebijakan ini 641
Detail kebijakan 641
Versi kebijakan 641
Dokumen kebijakan JSON 641
Pelajari selengkapnya 647
AmazonECSTaskExecutionRolePolicy 647
Menggunakan kebijakan ini 647
Detail kebijakan 647
Versi kebijakan 648
Dokumen kebijakan JSON 648
Pelajari selengkapnya 648
AmazonEFSCSIDriverPolicy 648
Menggunakan kebijakan ini 649
Detail kebijakan 649
Versi kebijakan 649
Dokumen kebijakan JSON 649
Pelajari selengkapnya 651

AmazonEKS_CNI_Policy 651
Menggunakan kebijakan ini 651
Detail kebijakan 651
Versi kebijakan 651
Dokumen kebijakan JSON 652
Pelajari selengkapnya 652
AmazonEKSBlockStoragePolicy 653
Menggunakan kebijakan ini 653
Detail kebijakan 653
Versi kebijakan 653
Dokumen kebijakan JSON 653
Pelajari selengkapnya 656
AmazonEKSBlockStoragePolicyV2 656
Menggunakan kebijakan ini 656
Detail kebijakan 656
Versi kebijakan 656
Dokumen kebijakan JSON 656
Pelajari selengkapnya 659
AmazonEKSClusterPolicy 659
Menggunakan kebijakan ini 659
Detail kebijakan 660
Versi kebijakan 660
Dokumen kebijakan JSON 660
Pelajari selengkapnya 662
AmazonEKSComputePolicy 662
Menggunakan kebijakan ini 663
Detail kebijakan 663
Versi kebijakan 663
Dokumen kebijakan JSON 663
Pelajari selengkapnya 666
AmazonEKSConnectorServiceRolePolicy 666
Menggunakan kebijakan ini 666
Detail kebijakan 666
Versi kebijakan 667
Dokumen kebijakan JSON 667
Pelajari selengkapnya 669

AmazonEKSDashboardConsoleReadOnly 669
Menggunakan kebijakan ini 669
Detail kebijakan 669
Versi kebijakan 669
Dokumen kebijakan JSON 670
Pelajari selengkapnya 671
AmazonEKSDashboardServiceRolePolicy 671
Menggunakan kebijakan ini 671
Detail kebijakan 671
Versi kebijakan 671
Dokumen kebijakan JSON 672
Pelajari selengkapnya 672
AmazonEKSFargatePodExecutionRolePolicy 672
Menggunakan kebijakan ini 673
Detail kebijakan 673
Versi kebijakan 673
Dokumen kebijakan JSON 673
Pelajari selengkapnya 674
AmazonEKSForFargateServiceRolePolicy 674
Menggunakan kebijakan ini 674
Detail kebijakan 674
Versi kebijakan 674
Dokumen kebijakan JSON 675
Pelajari selengkapnya 675
AmazonEKSLoadBalancingPolicy 675
Menggunakan kebijakan ini 675
Detail kebijakan 676
Versi kebijakan 676
Dokumen kebijakan JSON 676
Pelajari selengkapnya 682
AmazonEKSLocalOutpostClusterPolicy 682
Menggunakan kebijakan ini 682
Detail kebijakan 682
Versi kebijakan 682
Dokumen kebijakan JSON 682
Pelajari selengkapnya 684

AmazonEKSLocalOutpostServiceRolePolicy 684
Menggunakan kebijakan ini 685
Detail kebijakan 685
Versi kebijakan 685
Dokumen kebijakan JSON 685
Pelajari selengkapnya 691
AmazonEKSMCPReadOnlyAccess 691
Menggunakan kebijakan ini 691
Detail kebijakan 691
Versi kebijakan 692
Dokumen kebijakan JSON 692
Pelajari selengkapnya 694
AmazonEKSNetworkingPolicy 694
Menggunakan kebijakan ini 694
Detail kebijakan 694
Versi kebijakan 694
Dokumen kebijakan JSON 694
Pelajari selengkapnya 697
AmazonEKSServicePolicy 697
Menggunakan kebijakan ini 697
Detail kebijakan 697
Versi kebijakan 697
Dokumen kebijakan JSON 697
Pelajari selengkapnya 699
AmazonEKSServiceRolePolicy 700
Menggunakan kebijakan ini 700
Detail kebijakan 700
Versi kebijakan 700
Dokumen kebijakan JSON 700
Pelajari selengkapnya 709
AmazonEKSVPCResourceController 709
Menggunakan kebijakan ini 709
Detail kebijakan 709
Versi kebijakan 709
Dokumen kebijakan JSON 709
Pelajari selengkapnya 710

AmazonEKSWorkerNodeMinimalPolicy 710
Menggunakan kebijakan ini 711
Detail kebijakan 711
Versi kebijakan 711
Dokumen kebijakan JSON 711
Pelajari selengkapnya 711
AmazonEKSWorkerNodePolicy 712
Menggunakan kebijakan ini 712
Detail kebijakan 712
Versi kebijakan 712
Dokumen kebijakan JSON 712
Pelajari selengkapnya 713
AmazonElastiCacheFullAccess 713
Menggunakan kebijakan ini 713
Detail kebijakan 713
Versi kebijakan 714
Dokumen kebijakan JSON 714
Pelajari selengkapnya 717
AmazonElastiCacheReadOnlyAccess 717
Menggunakan kebijakan ini 717
Detail kebijakan 717
Versi kebijakan 718
Dokumen kebijakan JSON 718
Pelajari selengkapnya 718
AmazonElasticContainerRegistryPublicFullAccess 718
Menggunakan kebijakan ini 719
Detail kebijakan 719
Versi kebijakan 719
Dokumen kebijakan JSON 719
Pelajari selengkapnya 720
AmazonElasticContainerRegistryPublicPowerUser 720
Menggunakan kebijakan ini 720
Detail kebijakan 720
Versi kebijakan 720
Dokumen kebijakan JSON 721
Pelajari selengkapnya 721

AmazonElasticContainerRegistryPublicReadOnly 721
Menggunakan kebijakan ini 722
Detail kebijakan 722
Versi kebijakan 722
Dokumen kebijakan JSON 722
Pelajari selengkapnya 723
AmazonElasticFileSystemClientFullAccess 723
Menggunakan kebijakan ini 723
Detail kebijakan 723
Versi kebijakan 723
Dokumen kebijakan JSON 724
Pelajari selengkapnya 724
AmazonElasticFileSystemClientReadOnlyAccess 724
Menggunakan kebijakan ini 724
Detail kebijakan 724
Versi kebijakan 725
Dokumen kebijakan JSON 725
Pelajari selengkapnya 725
AmazonElasticFileSystemClientReadWriteAccess 725
Menggunakan kebijakan ini 726
Detail kebijakan 726
Versi kebijakan 726
Dokumen kebijakan JSON 726
Pelajari selengkapnya 727
AmazonElasticFileSystemFullAccess 727
Menggunakan kebijakan ini 727
Detail kebijakan 727
Versi kebijakan 727
Dokumen kebijakan JSON 727
Pelajari selengkapnya 729
AmazonElasticFileSystemReadOnlyAccess 730
Menggunakan kebijakan ini 730
Detail kebijakan 730
Versi kebijakan 730
Dokumen kebijakan JSON 730
Pelajari selengkapnya 731

AmazonElasticFileSystemServiceRolePolicy 731
Menggunakan kebijakan ini 732
Detail kebijakan 732
Versi kebijakan 732
Dokumen kebijakan JSON 732
Pelajari selengkapnya 734
AmazonElasticFileSystemsUtils 734
Menggunakan kebijakan ini 735
Detail kebijakan 735
Versi kebijakan 735
Dokumen kebijakan JSON 735
Pelajari selengkapnya 737
AmazonElasticMapReduceEditorsRole 737
Menggunakan kebijakan ini 738
Detail kebijakan 738
Versi kebijakan 738
Dokumen kebijakan JSON 738
Pelajari selengkapnya 739
AmazonElasticMapReduceforAutoScalingRole 739
Menggunakan kebijakan ini 740
Detail kebijakan 740
Versi kebijakan 740
Dokumen kebijakan JSON 740
Pelajari selengkapnya 741
AmazonElasticMapReduceforEC2Role 741
Menggunakan kebijakan ini 741
Detail kebijakan 741
Versi kebijakan 741
Dokumen kebijakan JSON 741
Pelajari selengkapnya 743
AmazonElasticMapReduceFullAccess 743
Menggunakan kebijakan ini 743
Detail kebijakan 743
Versi kebijakan 744
Dokumen kebijakan JSON 744
Pelajari selengkapnya 746

AmazonElasticMapReducePlacementGroupPolicy 746
Menggunakan kebijakan ini 746
Detail kebijakan 746
Versi kebijakan 746
Dokumen kebijakan JSON 747
Pelajari selengkapnya 747
AmazonElasticMapReduceReadOnlyAccess 747
Menggunakan kebijakan ini 748
Detail kebijakan 748
Versi kebijakan 748
Dokumen kebijakan JSON 748
Pelajari selengkapnya 749
AmazonElasticMapReduceRole 749
Menggunakan kebijakan ini 749
Detail kebijakan 749
Versi kebijakan 749
Dokumen kebijakan JSON 750
Pelajari selengkapnya 752
AmazonElasticsearchServiceRolePolicy 752
Menggunakan kebijakan ini 752
Detail kebijakan 752
Versi kebijakan 752
Dokumen kebijakan JSON 753
Pelajari selengkapnya 756
AmazonElasticTranscoder_FullAccess 756
Menggunakan kebijakan ini 756
Detail kebijakan 756
Versi kebijakan 756
Dokumen kebijakan JSON 756
Pelajari selengkapnya 757
AmazonElasticTranscoder_JobsSubmitter 757
Menggunakan kebijakan ini 758
Detail kebijakan 758
Versi kebijakan 758
Dokumen kebijakan JSON 758
Pelajari selengkapnya 759

AmazonElasticTranscoder_ReadOnlyAccess 759
Menggunakan kebijakan ini 759
Detail kebijakan 759
Versi kebijakan 759
Dokumen kebijakan JSON 760
Pelajari selengkapnya 760
AmazonElasticTranscoderRole 760
Menggunakan kebijakan ini 760
Detail kebijakan 761
Versi kebijakan 761
Dokumen kebijakan JSON 761
Pelajari selengkapnya 762
AmazonEMRCleanupPolicy 762
Menggunakan kebijakan ini 762
Detail kebijakan 762
Versi kebijakan 762
Dokumen kebijakan JSON 763
Pelajari selengkapnya 763
AmazonEMRContainersServiceRolePolicy 764
Menggunakan kebijakan ini 764
Detail kebijakan 764
Versi kebijakan 764
Dokumen kebijakan JSON 764
Pelajari selengkapnya 767
AmazonEMRFullAccessPolicy_v2 767
Menggunakan kebijakan ini 767
Detail kebijakan 767
Versi kebijakan 767
Dokumen kebijakan JSON 768
Pelajari selengkapnya 771
AmazonEMRReadOnlyAccessPolicy_v2 771
Menggunakan kebijakan ini 771
Detail kebijakan 771
Versi kebijakan 772
Dokumen kebijakan JSON 772
Pelajari selengkapnya 773

AmazonEMRServerlessServiceRolePolicy 773
Menggunakan kebijakan ini 773
Detail kebijakan 773
Versi kebijakan 774
Dokumen kebijakan JSON 774
Pelajari selengkapnya 775
AmazonEMRServicePolicy_v2 775
Menggunakan kebijakan ini 775
Detail kebijakan 775
Versi kebijakan 775
Dokumen kebijakan JSON 776
Pelajari selengkapnya 784
AmazonEMRServicePolicyForSessions 785
Menggunakan kebijakan ini 785
Detail kebijakan 785
Versi kebijakan 785
Dokumen kebijakan JSON 785
Pelajari selengkapnya 789
AmazonESCognitoAccess 789
Menggunakan kebijakan ini 789
Detail kebijakan 789
Versi kebijakan 790
Dokumen kebijakan JSON 790
Pelajari selengkapnya 791
AmazonESFullAccess 791
Menggunakan kebijakan ini 791
Detail kebijakan 791
Versi kebijakan 791
Dokumen kebijakan JSON 792
Pelajari selengkapnya 792
AmazonESReadOnlyAccess 792
Menggunakan kebijakan ini 792
Detail kebijakan 792
Versi kebijakan 793
Dokumen kebijakan JSON 793
Pelajari selengkapnya 793

AmazonEventBridgeApiDestinationsServiceRolePolicy 793
Menggunakan kebijakan ini 794
Detail kebijakan 794
Versi kebijakan 794
Dokumen kebijakan JSON 794
Pelajari selengkapnya 795
AmazonEventBridgeFullAccess 795
Menggunakan kebijakan ini 795
Detail kebijakan 796
Versi kebijakan 796
Dokumen kebijakan JSON 796
Pelajari selengkapnya 798
AmazonEventBridgePipesFullAccess 798
Menggunakan kebijakan ini 798
Detail kebijakan 799
Versi kebijakan 799
Dokumen kebijakan JSON 799
Pelajari selengkapnya 800
AmazonEventBridgePipesOperatorAccess 800
Menggunakan kebijakan ini 800
Detail kebijakan 800
Versi kebijakan 800
Dokumen kebijakan JSON 800
Pelajari selengkapnya 801
AmazonEventBridgePipesReadOnlyAccess 801
Menggunakan kebijakan ini 801
Detail kebijakan 801
Versi kebijakan 802
Dokumen kebijakan JSON 802
Pelajari selengkapnya 802
AmazonEventBridgeReadOnlyAccess 802
Menggunakan kebijakan ini 803
Detail kebijakan 803
Versi kebijakan 803
Dokumen kebijakan JSON 803
Pelajari selengkapnya 804

AmazonEventBridgeSchedulerFullAccess 805
Menggunakan kebijakan ini 805
Detail kebijakan 805
Versi kebijakan 805
Dokumen kebijakan JSON 805
Pelajari selengkapnya 806
AmazonEventBridgeSchedulerReadOnlyAccess 806
Menggunakan kebijakan ini 806
Detail kebijakan 806
Versi kebijakan 807
Dokumen kebijakan JSON 807
Pelajari selengkapnya 807
AmazonEventBridgeSchemasFullAccess 807
Menggunakan kebijakan ini 808
Detail kebijakan 808
Versi kebijakan 808
Dokumen kebijakan JSON 808
Pelajari selengkapnya 809
AmazonEventBridgeSchemasReadOnlyAccess 809
Menggunakan kebijakan ini 809
Detail kebijakan 809
Versi kebijakan 810
Dokumen kebijakan JSON 810
Pelajari selengkapnya 811
AmazonEventBridgeSchemasServiceRolePolicy 811
Menggunakan kebijakan ini 811
Detail kebijakan 811
Versi kebijakan 811
Dokumen kebijakan JSON 811
Pelajari selengkapnya 812
AmazonEVSServiceRolePolicy 812
Menggunakan kebijakan ini 812
Detail kebijakan 812
Versi kebijakan 813
Dokumen kebijakan JSON 813
Pelajari selengkapnya 818

AmazonFISServiceRolePolicy 818
Menggunakan kebijakan ini 818
Detail kebijakan 818
Versi kebijakan 819
Dokumen kebijakan JSON 819
Pelajari selengkapnya 820
AmazonForecastFullAccess 821
Menggunakan kebijakan ini 821
Detail kebijakan 821
Versi kebijakan 821
Dokumen kebijakan JSON 821
Pelajari selengkapnya 822
AmazonFraudDetectorFullAccessPolicy 822
Menggunakan kebijakan ini 822
Detail kebijakan 822
Versi kebijakan 823
Dokumen kebijakan JSON 823
Pelajari selengkapnya 824
AmazonFreeRTOSFullAccess 824
Menggunakan kebijakan ini 824
Detail kebijakan 824
Versi kebijakan 825
Dokumen kebijakan JSON 825
Pelajari selengkapnya 825
AmazonFreeRTOSOTAUpdate 825
Menggunakan kebijakan ini 825
Detail kebijakan 826
Versi kebijakan 826
Dokumen kebijakan JSON 826
Pelajari selengkapnya 827
AmazonFSxConsoleFullAccess 828
Menggunakan kebijakan ini 828
Detail kebijakan 828
Versi kebijakan 828
Dokumen kebijakan JSON 828
Pelajari selengkapnya 832

AmazonFSxConsoleReadOnlyAccess 832
Menggunakan kebijakan ini 832
Detail kebijakan 832
Versi kebijakan 832
Dokumen kebijakan JSON 833
Pelajari selengkapnya 833
AmazonFSxFullAccess 834
Menggunakan kebijakan ini 834
Detail kebijakan 834
Versi kebijakan 834
Dokumen kebijakan JSON 834
Pelajari selengkapnya 838
AmazonFSxReadOnlyAccess 838
Menggunakan kebijakan ini 839
Detail kebijakan 839
Versi kebijakan 839
Dokumen kebijakan JSON 839
Pelajari selengkapnya 839
AmazonFSxServiceRolePolicy 840
Menggunakan kebijakan ini 840
Detail kebijakan 840
Versi kebijakan 840
Dokumen kebijakan JSON 840
Pelajari selengkapnya 843
AmazonGlacierFullAccess 843
Menggunakan kebijakan ini 843
Detail kebijakan 844
Versi kebijakan 844
Dokumen kebijakan JSON 844
Pelajari selengkapnya 844
AmazonGlacierReadOnlyAccess 845
Menggunakan kebijakan ini 845
Detail kebijakan 845
Versi kebijakan 845
Dokumen kebijakan JSON 845
Pelajari selengkapnya 846

AmazonGrafanaAthenaAccess 846
Menggunakan kebijakan ini 846
Detail kebijakan 846
Versi kebijakan 847
Dokumen kebijakan JSON 847
Pelajari selengkapnya 848
AmazonGrafanaCloudWatchAccess 849
Menggunakan kebijakan ini 849
Detail kebijakan 849
Versi kebijakan 849
Dokumen kebijakan JSON 849
Pelajari selengkapnya 851
AmazonGrafanaRedshiftAccess 851
Menggunakan kebijakan ini 851
Detail kebijakan 851
Versi kebijakan 851
Dokumen kebijakan JSON 852
Pelajari selengkapnya 853
AmazonGrafanaServiceLinkedRolePolicy 853
Menggunakan kebijakan ini 853
Detail kebijakan 853
Versi kebijakan 854
Dokumen kebijakan JSON 854
Pelajari selengkapnya 855
AmazonGuardDutyFullAccess 855
Menggunakan kebijakan ini 855
Detail kebijakan 855
Versi kebijakan 856
Dokumen kebijakan JSON 856
Pelajari selengkapnya 857
AmazonGuardDutyFullAccess_v2 857
Menggunakan kebijakan ini 858
Detail kebijakan 858
Versi kebijakan 858
Dokumen kebijakan JSON 858
Pelajari selengkapnya 860

AmazonGuardDutyMalwareProtectionServiceRolePolicy 860
Menggunakan kebijakan ini 861
Detail kebijakan 861
Versi kebijakan 861
Dokumen kebijakan JSON 861
Pelajari selengkapnya 866
AmazonGuardDutyReadOnlyAccess 866
Menggunakan kebijakan ini 866
Detail kebijakan 866
Versi kebijakan 866
Dokumen kebijakan JSON 866
Pelajari selengkapnya 867
AmazonGuardDutyServiceRolePolicy 867
Menggunakan kebijakan ini 868
Detail kebijakan 868
Versi kebijakan 868
Dokumen kebijakan JSON 868
Pelajari selengkapnya 875
AmazonHealthLakeFullAccess 875
Menggunakan kebijakan ini 875
Detail kebijakan 875
Versi kebijakan 875
Dokumen kebijakan JSON 876
Pelajari selengkapnya 876
AmazonHealthLakeReadOnlyAccess 877
Menggunakan kebijakan ini 877
Detail kebijakan 877
Versi kebijakan 877
Dokumen kebijakan JSON 877
Pelajari selengkapnya 878
AmazonHoneycodeFullAccess 878
Menggunakan kebijakan ini 878
Detail kebijakan 878
Versi kebijakan 879
Dokumen kebijakan JSON 879
Pelajari selengkapnya 879

AmazonHoneycodeReadOnlyAccess 879
Menggunakan kebijakan ini 880
Detail kebijakan 880
Versi kebijakan 880
Dokumen kebijakan JSON 880
Pelajari selengkapnya 881
AmazonHoneycodeServiceRolePolicy 881
Menggunakan kebijakan ini 881
Detail kebijakan 881
Versi kebijakan 881
Dokumen kebijakan JSON 882
Pelajari selengkapnya 882
AmazonHoneycodeTeamAssociationFullAccess 882
Menggunakan kebijakan ini 882
Detail kebijakan 882
Versi kebijakan 883
Dokumen kebijakan JSON 883
Pelajari selengkapnya 883
AmazonHoneycodeTeamAssociationReadOnlyAccess 883
Menggunakan kebijakan ini 884
Detail kebijakan 884
Versi kebijakan 884
Dokumen kebijakan JSON 884
Pelajari selengkapnya 884
AmazonHoneycodeWorkbookFullAccess 885
Menggunakan kebijakan ini 885
Detail kebijakan 885
Versi kebijakan 885
Dokumen kebijakan JSON 885
Pelajari selengkapnya 886
AmazonHoneycodeWorkbookReadOnlyAccess 886
Menggunakan kebijakan ini 886
Detail kebijakan 886
Versi kebijakan 887
Dokumen kebijakan JSON 887
Pelajari selengkapnya 887

AmazonInspector2AgentlessServiceRolePolicy 888
Menggunakan kebijakan ini 888
Detail kebijakan 888
Versi kebijakan 888
Dokumen kebijakan JSON 888
Pelajari selengkapnya 893
AmazonInspector2AmiScanServiceRolePolicy 893
Menggunakan kebijakan ini 893
Detail kebijakan 893
Versi kebijakan 894
Dokumen kebijakan JSON 894
Pelajari selengkapnya 897
AmazonInspector2FullAccess 897
Menggunakan kebijakan ini 898
Detail kebijakan 898
Versi kebijakan 898
Dokumen kebijakan JSON 898
Pelajari selengkapnya 899
AmazonInspector2FullAccess_v2 900
Menggunakan kebijakan ini 900
Detail kebijakan 900
Versi kebijakan 900
Dokumen kebijakan JSON 900
Pelajari selengkapnya 903
AmazonInspector2ManagedCisPolicy 904
Menggunakan kebijakan ini 904
Detail kebijakan 904
Versi kebijakan 904
Dokumen kebijakan JSON 904
Pelajari selengkapnya 905
AmazonInspector2ManagedTelemetryPolicy 905
Menggunakan kebijakan ini 905
Detail kebijakan 905
Versi kebijakan 906
Dokumen kebijakan JSON 906
Pelajari selengkapnya 906

AmazonInspector2ReadOnlyAccess 906
Menggunakan kebijakan ini 907
Detail kebijakan 907
Versi kebijakan 907
Dokumen kebijakan JSON 907
Pelajari selengkapnya 909
AmazonInspector2ServiceRolePolicy 909
Menggunakan kebijakan ini 909
Detail kebijakan 909
Versi kebijakan 910
Dokumen kebijakan JSON 910
Pelajari selengkapnya 918
AmazonInspector2ThirdPartyServiceRolePolicy 918
Menggunakan kebijakan ini 918
Detail kebijakan 918
Versi kebijakan 918
Dokumen kebijakan JSON 919
Pelajari selengkapnya 923
AmazonInspectorFullAccess 923
Menggunakan kebijakan ini 924
Detail kebijakan 924
Versi kebijakan 924
Dokumen kebijakan JSON 924
Pelajari selengkapnya 925
AmazonInspectorReadOnlyAccess 925
Menggunakan kebijakan ini 926
Detail kebijakan 926
Versi kebijakan 926
Dokumen kebijakan JSON 926
Pelajari selengkapnya 927
AmazonInspectorServiceRolePolicy 927
Menggunakan kebijakan ini 927
Detail kebijakan 927
Versi kebijakan 927
Dokumen kebijakan JSON 928
Pelajari selengkapnya 929

AmazonKendraFullAccess 929
Menggunakan kebijakan ini 929
Detail kebijakan 929
Versi kebijakan 929
Dokumen kebijakan JSON 930
Pelajari selengkapnya 931
AmazonKendraReadOnlyAccess 932
Menggunakan kebijakan ini 932
Detail kebijakan 932
Versi kebijakan 932
Dokumen kebijakan JSON 932
Pelajari selengkapnya 933
AmazonKeyspacesFullAccess 933
Menggunakan kebijakan ini 933
Detail kebijakan 933
Versi kebijakan 933
Dokumen kebijakan JSON 934
Pelajari selengkapnya 936
AmazonKeyspacesReadOnlyAccess 936
Menggunakan kebijakan ini 936
Detail kebijakan 936
Versi kebijakan 936
Dokumen kebijakan JSON 937
Pelajari selengkapnya 937
AmazonKeyspacesReadOnlyAccess_v2 938
Menggunakan kebijakan ini 938
Detail kebijakan 938
Versi kebijakan 938
Dokumen kebijakan JSON 938
Pelajari selengkapnya 939
AmazonKinesisAnalyticsFullAccess 939
Menggunakan kebijakan ini 940
Detail kebijakan 940
Versi kebijakan 940
Dokumen kebijakan JSON 940
Pelajari selengkapnya 942

AmazonKinesisAnalyticsReadOnly 942
Menggunakan kebijakan ini 942
Detail kebijakan 942
Versi kebijakan 942
Dokumen kebijakan JSON 942
Pelajari selengkapnya 944
AmazonKinesisFirehoseFullAccess 944
Menggunakan kebijakan ini 944
Detail kebijakan 944
Versi kebijakan 944
Dokumen kebijakan JSON 945
Pelajari selengkapnya 945
AmazonKinesisFirehoseReadOnlyAccess 945
Menggunakan kebijakan ini 945
Detail kebijakan 946
Versi kebijakan 946
Dokumen kebijakan JSON 946
Pelajari selengkapnya 946
AmazonKinesisFullAccess 947
Menggunakan kebijakan ini 947
Detail kebijakan 947
Versi kebijakan 947
Dokumen kebijakan JSON 947
Pelajari selengkapnya 948
AmazonKinesisReadOnlyAccess 948
Menggunakan kebijakan ini 948
Detail kebijakan 948
Versi kebijakan 948
Dokumen kebijakan JSON 948
Pelajari selengkapnya 949
AmazonKinesisVideoStreamsFullAccess 949
Menggunakan kebijakan ini 949
Detail kebijakan 949
Versi kebijakan 950
Dokumen kebijakan JSON 950
Pelajari selengkapnya 950

AmazonKinesisVideoStreamsReadOnlyAccess 950
Menggunakan kebijakan ini 950
Detail kebijakan 951
Versi kebijakan 951
Dokumen kebijakan JSON 951
Pelajari selengkapnya 951
AmazonLaunchWizard_Fullaccess 952
Menggunakan kebijakan ini 952
Detail kebijakan 952
Versi kebijakan 952
Dokumen kebijakan JSON 952
Pelajari selengkapnya 966
AmazonLaunchWizardFullAccessV2 967
Menggunakan kebijakan ini 967
Detail kebijakan 967
Versi kebijakan 967
Dokumen kebijakan JSON 967
Pelajari selengkapnya 989
AmazonLexChannelsAccess 989
Menggunakan kebijakan ini 989
Detail kebijakan 989
Versi kebijakan 989
Dokumen kebijakan JSON 990
Pelajari selengkapnya 990
AmazonLexFullAccess 990
Menggunakan kebijakan ini 990
Detail kebijakan 990
Versi kebijakan 991
Dokumen kebijakan JSON 991
Pelajari selengkapnya 996
AmazonLexReadOnly 997
Menggunakan kebijakan ini 997
Detail kebijakan 997
Versi kebijakan 997
Dokumen kebijakan JSON 997
Pelajari selengkapnya 999

AmazonLexReplicationPolicy 999
Menggunakan kebijakan ini 999
Detail kebijakan 999
Versi kebijakan 999
Dokumen kebijakan JSON 1000
Pelajari selengkapnya 1002
AmazonLexRunBotsOnly 1002
Menggunakan kebijakan ini 1002
Detail kebijakan 1002
Versi kebijakan 1003
Dokumen kebijakan JSON 1003
Pelajari selengkapnya 1003
AmazonLexV2BotPolicy 1003
Menggunakan kebijakan ini 1004
Detail kebijakan 1004
Versi kebijakan 1004
Dokumen kebijakan JSON 1004
Pelajari selengkapnya 1005
AmazonLookoutEquipmentFullAccess 1005
Menggunakan kebijakan ini 1005
Detail kebijakan 1005
Versi kebijakan 1005
Dokumen kebijakan JSON 1005
Pelajari selengkapnya 1007
AmazonLookoutEquipmentReadOnlyAccess 1007
Menggunakan kebijakan ini 1007
Detail kebijakan 1007
Versi kebijakan 1007
Dokumen kebijakan JSON 1007
Pelajari selengkapnya 1008
AmazonLookoutMetricsFullAccess 1008
Menggunakan kebijakan ini 1008
Detail kebijakan 1008
Versi kebijakan 1009
Dokumen kebijakan JSON 1009
Pelajari selengkapnya 1009

AmazonLookoutMetricsReadOnlyAccess 1010
Menggunakan kebijakan ini 1010
Detail kebijakan 1010
Versi kebijakan 1010
Dokumen kebijakan JSON 1010
Pelajari selengkapnya 1011
AmazonLookoutVisionConsoleFullAccess 1011
Menggunakan kebijakan ini 1011
Detail kebijakan 1011
Versi kebijakan 1012
Dokumen kebijakan JSON 1012
Pelajari selengkapnya 1014
AmazonLookoutVisionConsoleReadOnlyAccess 1014
Menggunakan kebijakan ini 1014
Detail kebijakan 1014
Versi kebijakan 1015
Dokumen kebijakan JSON 1015
Pelajari selengkapnya 1016
AmazonLookoutVisionFullAccess 1016
Menggunakan kebijakan ini 1017
Detail kebijakan 1017
Versi kebijakan 1017
Dokumen kebijakan JSON 1017
Pelajari selengkapnya 1017
AmazonLookoutVisionReadOnlyAccess 1018
Menggunakan kebijakan ini 1018
Detail kebijakan 1018
Versi kebijakan 1018
Dokumen kebijakan JSON 1018
Pelajari selengkapnya 1019
AmazonMachineLearningBatchPredictionsAccess 1019
Menggunakan kebijakan ini 1019
Detail kebijakan 1019
Versi kebijakan 1020
Dokumen kebijakan JSON 1020
Pelajari selengkapnya 1020

AmazonMachineLearningCreateOnlyAccess 1021
Menggunakan kebijakan ini 1021
Detail kebijakan 1021
Versi kebijakan 1021
Dokumen kebijakan JSON 1021
Pelajari selengkapnya 1022
AmazonMachineLearningFullAccess 1022
Menggunakan kebijakan ini 1022
Detail kebijakan 1022
Versi kebijakan 1022
Dokumen kebijakan JSON 1023
Pelajari selengkapnya 1023
AmazonMachineLearningManageRealTimeEndpointOnlyAccess 1023
Menggunakan kebijakan ini 1023
Detail kebijakan 1023
Versi kebijakan 1024
Dokumen kebijakan JSON 1024
Pelajari selengkapnya 1024
AmazonMachineLearningReadOnlyAccess 1024
Menggunakan kebijakan ini 1025
Detail kebijakan 1025
Versi kebijakan 1025
Dokumen kebijakan JSON 1025
Pelajari selengkapnya 1026
AmazonMachineLearningRealTimePredictionOnlyAccess 1026
Menggunakan kebijakan ini 1026
Detail kebijakan 1026
Versi kebijakan 1026
Dokumen kebijakan JSON 1027
Pelajari selengkapnya 1027
AmazonMachineLearningRoleforRedshiftDataSourceV3 1027
Menggunakan kebijakan ini 1027
Detail kebijakan 1027
Versi kebijakan 1028
Dokumen kebijakan JSON 1028
Pelajari selengkapnya 1029

AmazonMacieFullAccess 1029
Menggunakan kebijakan ini 1029
Detail kebijakan 1029
Versi kebijakan 1029
Dokumen kebijakan JSON 1030
Pelajari selengkapnya 1030
AmazonMacieHandshakeRole 1031
Menggunakan kebijakan ini 1031
Detail kebijakan 1031
Versi kebijakan 1031
Dokumen kebijakan JSON 1031
Pelajari selengkapnya 1032
AmazonMacieReadOnlyAccess 1032
Menggunakan kebijakan ini 1032
Detail kebijakan 1032
Versi kebijakan 1032
Dokumen kebijakan JSON 1033
Pelajari selengkapnya 1033
AmazonMacieServiceRole 1033
Menggunakan kebijakan ini 1033
Detail kebijakan 1034
Versi kebijakan 1034
Dokumen kebijakan JSON 1034
Pelajari selengkapnya 1034
AmazonMacieServiceRolePolicy 1035
Menggunakan kebijakan ini 1035
Detail kebijakan 1035
Versi kebijakan 1035
Dokumen kebijakan JSON 1035
Pelajari selengkapnya 1037
AmazonManagedBlockchainConsoleFullAccess 1037
Menggunakan kebijakan ini 1037
Detail kebijakan 1037
Versi kebijakan 1037
Dokumen kebijakan JSON 1037
Pelajari selengkapnya 1038

AmazonManagedBlockchainFullAccess 1038
Menggunakan kebijakan ini 1038
Detail kebijakan 1038
Versi kebijakan 1039
Dokumen kebijakan JSON 1039
Pelajari selengkapnya 1039
AmazonManagedBlockchainReadOnlyAccess 1039
Menggunakan kebijakan ini 1040
Detail kebijakan 1040
Versi kebijakan 1040
Dokumen kebijakan JSON 1040
Pelajari selengkapnya 1041
AmazonManagedBlockchainServiceRolePolicy 1041
Menggunakan kebijakan ini 1041
Detail kebijakan 1041
Versi kebijakan 1041
Dokumen kebijakan JSON 1042
Pelajari selengkapnya 1042
AmazonMCSFullAccess 1042
Menggunakan kebijakan ini 1042
Detail kebijakan 1043
Versi kebijakan 1043
Dokumen kebijakan JSON 1043
Pelajari selengkapnya 1044
AmazonMCSReadOnlyAccess 1044
Menggunakan kebijakan ini 1045
Detail kebijakan 1045
Versi kebijakan 1045
Dokumen kebijakan JSON 1045
Pelajari selengkapnya 1046
AmazonMechanicalTurkFullAccess 1046
Menggunakan kebijakan ini 1046
Detail kebijakan 1046
Versi kebijakan 1046
Dokumen kebijakan JSON 1047
Pelajari selengkapnya 1047

AmazonMechanicalTurkReadOnly 1047
Menggunakan kebijakan ini 1047
Detail kebijakan 1047
Versi kebijakan 1048
Dokumen kebijakan JSON 1048
Pelajari selengkapnya 1048
AmazonMemoryDBFullAccess 1048
Menggunakan kebijakan ini 1049
Detail kebijakan 1049
Versi kebijakan 1049
Dokumen kebijakan JSON 1049
Pelajari selengkapnya 1050
AmazonMemoryDBReadOnlyAccess 1050
Menggunakan kebijakan ini 1050
Detail kebijakan 1050
Versi kebijakan 1050
Dokumen kebijakan JSON 1051
Pelajari selengkapnya 1051
AmazonMobileAnalyticsFinancialReportAccess 1051
Menggunakan kebijakan ini 1051
Detail kebijakan 1051
Versi kebijakan 1052
Dokumen kebijakan JSON 1052
Pelajari selengkapnya 1052
AmazonMobileAnalyticsFullAccess 1052
Menggunakan kebijakan ini 1053
Detail kebijakan 1053
Versi kebijakan 1053
Dokumen kebijakan JSON 1053
Pelajari selengkapnya 1053
AmazonMobileAnalyticsNon-financialReportAccess 1054
Menggunakan kebijakan ini 1054
Detail kebijakan 1054
Versi kebijakan 1054
Dokumen kebijakan JSON 1054
Pelajari selengkapnya 1055

AmazonMobileAnalyticsWriteOnlyAccess 1055
Menggunakan kebijakan ini 1055
Detail kebijakan 1055
Versi kebijakan 1055
Dokumen kebijakan JSON 1056
Pelajari selengkapnya 1056
AmazonMonitronFullAccess 1056
Menggunakan kebijakan ini 1056
Detail kebijakan 1056
Versi kebijakan 1057
Dokumen kebijakan JSON 1057
Pelajari selengkapnya 1059
AmazonMQApiFullAccess 1059
Menggunakan kebijakan ini 1059
Detail kebijakan 1059
Versi kebijakan 1059
Dokumen kebijakan JSON 1059
Pelajari selengkapnya 1061
AmazonMQApiReadOnlyAccess 1061
Menggunakan kebijakan ini 1061
Detail kebijakan 1061
Versi kebijakan 1061
Dokumen kebijakan JSON 1061
Pelajari selengkapnya 1062
AmazonMQFullAccess 1062
Menggunakan kebijakan ini 1062
Detail kebijakan 1062
Versi kebijakan 1063
Dokumen kebijakan JSON 1063
Pelajari selengkapnya 1064
AmazonMQReadOnlyAccess 1065
Menggunakan kebijakan ini 1065
Detail kebijakan 1065
Versi kebijakan 1065
Dokumen kebijakan JSON 1065
Pelajari selengkapnya 1066

AmazonMQServiceRolePolicy 1066
Menggunakan kebijakan ini 1066
Detail kebijakan 1066
Versi kebijakan 1066
Dokumen kebijakan JSON 1067
Pelajari selengkapnya 1068
AmazonMSKConnectReadOnlyAccess 1069
Menggunakan kebijakan ini 1069
Detail kebijakan 1069
Versi kebijakan 1069
Dokumen kebijakan JSON 1069
Pelajari selengkapnya 1070
AmazonMSKFullAccess 1071
Menggunakan kebijakan ini 1071
Detail kebijakan 1071
Versi kebijakan 1071
Dokumen kebijakan JSON 1071
Pelajari selengkapnya 1074
AmazonMSKReadOnlyAccess 1074
Menggunakan kebijakan ini 1074
Detail kebijakan 1074
Versi kebijakan 1075
Dokumen kebijakan JSON 1075
Pelajari selengkapnya 1075
AmazonMWAAServerlessServiceRolePolicy 1076
Menggunakan kebijakan ini 1076
Detail kebijakan 1076
Versi kebijakan 1076
Dokumen kebijakan JSON 1076
Pelajari selengkapnya 1077
AmazonMWAAServiceRolePolicy 1077
Menggunakan kebijakan ini 1077
Detail kebijakan 1077
Versi kebijakan 1078
Dokumen kebijakan JSON 1078
Pelajari selengkapnya 1080

AmazonNimbleStudio-LaunchProfileWorker 1080
Menggunakan kebijakan ini 1080
Detail kebijakan 1080
Versi kebijakan 1081
Dokumen kebijakan JSON 1081
Pelajari selengkapnya 1081
AmazonNimbleStudio-StudioAdmin 1082
Menggunakan kebijakan ini 1082
Detail kebijakan 1082
Versi kebijakan 1082
Dokumen kebijakan JSON 1082
Pelajari selengkapnya 1084
AmazonNimbleStudio-StudioUser 1084
Menggunakan kebijakan ini 1085
Detail kebijakan 1085
Versi kebijakan 1085
Dokumen kebijakan JSON 1085
Pelajari selengkapnya 1087
AmazonODBAutonomousDatabaseAdmin 1087
Menggunakan kebijakan ini 1088
Detail kebijakan 1088
Versi kebijakan 1088
Dokumen kebijakan JSON 1088
Pelajari selengkapnya 1090
AmazonODBAutonomousVmClusterAdmin 1090
Menggunakan kebijakan ini 1091
Detail kebijakan 1091
Versi kebijakan 1091
Dokumen kebijakan JSON 1091
Pelajari selengkapnya 1093
AmazonODBExadataInfrastructureAdmin 1093
Menggunakan kebijakan ini 1093
Detail kebijakan 1093
Versi kebijakan 1093
Dokumen kebijakan JSON 1094
Pelajari selengkapnya 1095

AmazonODBExadataVmClusterAdmin 1095
Menggunakan kebijakan ini 1096
Detail kebijakan 1096
Versi kebijakan 1096
Dokumen kebijakan JSON 1096
Pelajari selengkapnya 1098
AmazonODBExascaleStorageVaultAdmin 1098
Menggunakan kebijakan ini 1098
Detail kebijakan 1098
Versi kebijakan 1099
Dokumen kebijakan JSON 1099
Pelajari selengkapnya 1100
AmazonODBExascaleVmClusterAdmin 1101
Menggunakan kebijakan ini 1101
Detail kebijakan 1101
Versi kebijakan 1101
Dokumen kebijakan JSON 1101
Pelajari selengkapnya 1103
AmazonODBFullAccess 1103
Menggunakan kebijakan ini 1103
Detail kebijakan 1103
Versi kebijakan 1104
Dokumen kebijakan JSON 1104
Pelajari selengkapnya 1107
AmazonODBNetworkAdmin 1107
Menggunakan kebijakan ini 1107
Detail kebijakan 1107
Versi kebijakan 1108
Dokumen kebijakan JSON 1108
Pelajari selengkapnya 1110
AmazonODBReadOnlyAccess 1110
Menggunakan kebijakan ini 1110
Detail kebijakan 1110
Versi kebijakan 1110
Dokumen kebijakan JSON 1111
Pelajari selengkapnya 1112

AmazonODBServiceRolePolicy 1112
Menggunakan kebijakan ini 1112
Detail kebijakan 1112
Versi kebijakan 1113
Dokumen kebijakan JSON 1113
Pelajari selengkapnya 1114
AmazonOmicsFullAccess 1114
Menggunakan kebijakan ini 1115
Detail kebijakan 1115
Versi kebijakan 1115
Dokumen kebijakan JSON 1115
Pelajari selengkapnya 1116
AmazonOmicsReadOnlyAccess 1116
Menggunakan kebijakan ini 1116
Detail kebijakan 1116
Versi kebijakan 1117
Dokumen kebijakan JSON 1117
Pelajari selengkapnya 1117
AmazonOneEnterpriseFullAccess 1117
Menggunakan kebijakan ini 1118
Detail kebijakan 1118
Versi kebijakan 1118
Dokumen kebijakan JSON 1118
Pelajari selengkapnya 1118
AmazonOneEnterpriseInstallerAccess 1119
Menggunakan kebijakan ini 1119
Detail kebijakan 1119
Versi kebijakan 1119
Dokumen kebijakan JSON 1119
Pelajari selengkapnya 1120
AmazonOneEnterpriseReadOnlyAccess 1120
Menggunakan kebijakan ini 1120
Detail kebijakan 1120
Versi kebijakan 1121
Dokumen kebijakan JSON 1121
Pelajari selengkapnya 1121

AmazonOpenSearchDashboardsServiceRolePolicy 1121
Menggunakan kebijakan ini 1122
Detail kebijakan 1122
Versi kebijakan 1122
Dokumen kebijakan JSON 1122
Pelajari selengkapnya 1123
AmazonOpenSearchDirectQueryGlueCreateAccess 1123
Menggunakan kebijakan ini 1123
Detail kebijakan 1123
Versi kebijakan 1123
Dokumen kebijakan JSON 1123
Pelajari selengkapnya 1124
AmazonOpenSearchIngestionFullAccess 1124
Menggunakan kebijakan ini 1124
Detail kebijakan 1124
Versi kebijakan 1125
Dokumen kebijakan JSON 1125
Pelajari selengkapnya 1126
AmazonOpenSearchIngestionReadOnlyAccess 1126
Menggunakan kebijakan ini 1126
Detail kebijakan 1126
Versi kebijakan 1126
Dokumen kebijakan JSON 1127
Pelajari selengkapnya 1127
AmazonOpenSearchIngestionServiceRolePolicy 1127
Menggunakan kebijakan ini 1127
Detail kebijakan 1128
Versi kebijakan 1128
Dokumen kebijakan JSON 1128
Pelajari selengkapnya 1130
AmazonOpenSearchServerlessServiceRolePolicy 1130
Menggunakan kebijakan ini 1130
Detail kebijakan 1130
Versi kebijakan 1130
Dokumen kebijakan JSON 1131
Pelajari selengkapnya 1131

AmazonOpenSearchServiceCognitoAccess 1131
Menggunakan kebijakan ini 1131
Detail kebijakan 1132
Versi kebijakan 1132
Dokumen kebijakan JSON 1132
Pelajari selengkapnya 1133
AmazonOpenSearchServiceFullAccess 1133
Menggunakan kebijakan ini 1133
Detail kebijakan 1134
Versi kebijakan 1134
Dokumen kebijakan JSON 1134
Pelajari selengkapnya 1134
AmazonOpenSearchServiceReadOnlyAccess 1135
Menggunakan kebijakan ini 1135
Detail kebijakan 1135
Versi kebijakan 1135
Dokumen kebijakan JSON 1135
Pelajari selengkapnya 1136
AmazonOpenSearchServiceRolePolicy 1136
Menggunakan kebijakan ini 1136
Detail kebijakan 1136
Versi kebijakan 1136
Dokumen kebijakan JSON 1137
Pelajari selengkapnya 1141
AmazonPersonalizeFullAccess 1142
Menggunakan kebijakan ini 1142
Detail kebijakan 1142
Versi kebijakan 1142
Dokumen kebijakan JSON 1142
Pelajari selengkapnya 1143
AmazonPollyFullAccess 1144
Menggunakan kebijakan ini 1144
Detail kebijakan 1144
Versi kebijakan 1144
Dokumen kebijakan JSON 1144
Pelajari selengkapnya 1145

AmazonPollyReadOnlyAccess 1145
Menggunakan kebijakan ini 1145
Detail kebijakan 1145
Versi kebijakan 1145
Dokumen kebijakan JSON 1146
Pelajari selengkapnya 1146
AmazonPrometheusConsoleFullAccess 1146
Menggunakan kebijakan ini 1146
Detail kebijakan 1147
Versi kebijakan 1147
Dokumen kebijakan JSON 1147
Pelajari selengkapnya 1148
AmazonPrometheusFullAccess 1148
Menggunakan kebijakan ini 1148
Detail kebijakan 1149
Versi kebijakan 1149
Dokumen kebijakan JSON 1149
Pelajari selengkapnya 1150
AmazonPrometheusQueryAccess 1150
Menggunakan kebijakan ini 1150
Detail kebijakan 1151
Versi kebijakan 1151
Dokumen kebijakan JSON 1151
Pelajari selengkapnya 1151
AmazonPrometheusRemoteWriteAccess 1152
Menggunakan kebijakan ini 1152
Detail kebijakan 1152
Versi kebijakan 1152
Dokumen kebijakan JSON 1152
Pelajari selengkapnya 1153
AmazonPrometheusScraperServiceRolePolicy 1153
Menggunakan kebijakan ini 1153
Detail kebijakan 1153
Versi kebijakan 1153
Dokumen kebijakan JSON 1154
Pelajari selengkapnya 1156

AmazonQDeveloperAccess 1156
Menggunakan kebijakan ini 1157
Detail kebijakan 1157
Versi kebijakan 1157
Dokumen kebijakan JSON 1157
Pelajari selengkapnya 1158
AmazonQFullAccess 1159
Menggunakan kebijakan ini 1159
Detail kebijakan 1159
Versi kebijakan 1159
Dokumen kebijakan JSON 1159
Pelajari selengkapnya 1161
AmazonQLDBConsoleFullAccess 1161
Menggunakan kebijakan ini 1161
Detail kebijakan 1162
Versi kebijakan 1162
Dokumen kebijakan JSON 1162
Pelajari selengkapnya 1164
AmazonQLDBFullAccess 1164
Menggunakan kebijakan ini 1164
Detail kebijakan 1164
Versi kebijakan 1164
Dokumen kebijakan JSON 1165
Pelajari selengkapnya 1166
AmazonQLDBReadOnly 1166
Menggunakan kebijakan ini 1166
Detail kebijakan 1166
Versi kebijakan 1167
Dokumen kebijakan JSON 1167
Pelajari selengkapnya 1167
AmazonRDSBetaServiceRolePolicy 1168
Menggunakan kebijakan ini 1168
Detail kebijakan 1168
Versi kebijakan 1168
Dokumen kebijakan JSON 1168
Pelajari selengkapnya 1171

AmazonRDSCustomInstanceProfileRolePolicy 1171
Menggunakan kebijakan ini 1172
Detail kebijakan 1172
Versi kebijakan 1172
Dokumen kebijakan JSON 1172
Pelajari selengkapnya 1179
AmazonRDSCustomPreviewServiceRolePolicy 1179
Menggunakan kebijakan ini 1180
Detail kebijakan 1180
Versi kebijakan 1180
Dokumen kebijakan JSON 1180
Pelajari selengkapnya 1198
AmazonRDSCustomServiceRolePolicy 1198
Menggunakan kebijakan ini 1198
Detail kebijakan 1198
Versi kebijakan 1198
Dokumen kebijakan JSON 1198
Pelajari selengkapnya 1217
AmazonRDSDataFullAccess 1218
Menggunakan kebijakan ini 1218
Detail kebijakan 1218
Versi kebijakan 1218
Dokumen kebijakan JSON 1218
Pelajari selengkapnya 1219
AmazonRDSDirectoryServiceAccess 1220
Menggunakan kebijakan ini 1220
Detail kebijakan 1220
Versi kebijakan 1220
Dokumen kebijakan JSON 1220
Pelajari selengkapnya 1221
AmazonRDSEnhancedMonitoringRole 1221
Menggunakan kebijakan ini 1221
Detail kebijakan 1221
Versi kebijakan 1221
Dokumen kebijakan JSON 1222
Pelajari selengkapnya 1222

AmazonRDSFullAccess 1223
Menggunakan kebijakan ini 1223
Detail kebijakan 1223
Versi kebijakan 1223
Dokumen kebijakan JSON 1223
Pelajari selengkapnya 1225
AmazonRDSPerformanceInsightsFullAccess 1225
Menggunakan kebijakan ini 1226
Detail kebijakan 1226
Versi kebijakan 1226
Dokumen kebijakan JSON 1226
Pelajari selengkapnya 1228
AmazonRDSPerformanceInsightsReadOnly 1228
Menggunakan kebijakan ini 1228
Detail kebijakan 1228
Versi kebijakan 1228
Dokumen kebijakan JSON 1229
Pelajari selengkapnya 1231
AmazonRDSPreviewServiceRolePolicy 1231
Menggunakan kebijakan ini 1231
Detail kebijakan 1231
Versi kebijakan 1232
Dokumen kebijakan JSON 1232
Pelajari selengkapnya 1235
AmazonRDSReadOnlyAccess 1235
Menggunakan kebijakan ini 1235
Detail kebijakan 1235
Versi kebijakan 1235
Dokumen kebijakan JSON 1236
Pelajari selengkapnya 1237
AmazonRDSServiceRolePolicy 1237
Menggunakan kebijakan ini 1237
Detail kebijakan 1237
Versi kebijakan 1237
Dokumen kebijakan JSON 1238
Pelajari selengkapnya 1241

AmazonRedshiftAllCommandsFullAccess 1242
Menggunakan kebijakan ini 1242
Detail kebijakan 1242
Versi kebijakan 1242
Dokumen kebijakan JSON 1242
Pelajari selengkapnya 1248
AmazonRedshiftDataFullAccess 1248
Menggunakan kebijakan ini 1248
Detail kebijakan 1248
Versi kebijakan 1248
Dokumen kebijakan JSON 1248
Pelajari selengkapnya 1250
AmazonRedshiftFederatedAuthorization 1251
Menggunakan kebijakan ini 1251
Detail kebijakan 1251
Versi kebijakan 1251
Dokumen kebijakan JSON 1251
Pelajari selengkapnya 1252
AmazonRedshiftFullAccess 1253
Menggunakan kebijakan ini 1253
Detail kebijakan 1253
Versi kebijakan 1253
Dokumen kebijakan JSON 1253
Pelajari selengkapnya 1255
AmazonRedshiftQueryEditor 1255
Menggunakan kebijakan ini 1256
Detail kebijakan 1256
Versi kebijakan 1256
Dokumen kebijakan JSON 1256
Pelajari selengkapnya 1258
AmazonRedshiftQueryEditorV2FullAccess 1258
Menggunakan kebijakan ini 1258
Detail kebijakan 1259
Versi kebijakan 1259
Dokumen kebijakan JSON 1259
Pelajari selengkapnya 1260

AmazonRedshiftQueryEditorV2NoSharing 1261
Menggunakan kebijakan ini 1261
Detail kebijakan 1261
Versi kebijakan 1261
Dokumen kebijakan JSON 1261
Pelajari selengkapnya 1265
AmazonRedshiftQueryEditorV2ReadSharing 1265
Menggunakan kebijakan ini 1265
Detail kebijakan 1266
Versi kebijakan 1266
Dokumen kebijakan JSON 1266
Pelajari selengkapnya 1271
AmazonRedshiftQueryEditorV2ReadWriteSharing 1271
Menggunakan kebijakan ini 1271
Detail kebijakan 1271
Versi kebijakan 1272
Dokumen kebijakan JSON 1272
Pelajari selengkapnya 1277
AmazonRedshiftReadOnlyAccess 1277
Menggunakan kebijakan ini 1277
Detail kebijakan 1277
Versi kebijakan 1277
Dokumen kebijakan JSON 1278
Pelajari selengkapnya 1278
AmazonRedshiftServiceLinkedRolePolicy 1279
Menggunakan kebijakan ini 1279
Detail kebijakan 1279
Versi kebijakan 1279
Dokumen kebijakan JSON 1279
Pelajari selengkapnya 1286
AmazonRekognitionCustomLabelsFullAccess 1286
Menggunakan kebijakan ini 1286
Detail kebijakan 1286
Versi kebijakan 1286
Dokumen kebijakan JSON 1286
Pelajari selengkapnya 1288

AmazonRekognitionFullAccess 1288
Menggunakan kebijakan ini 1288
Detail kebijakan 1288
Versi kebijakan 1288
Dokumen kebijakan JSON 1288
Pelajari selengkapnya 1289
AmazonRekognitionReadOnlyAccess 1289
Menggunakan kebijakan ini 1289
Detail kebijakan 1289
Versi kebijakan 1290
Dokumen kebijakan JSON 1290
Pelajari selengkapnya 1291
AmazonRekognitionServiceRole 1291
Menggunakan kebijakan ini 1291
Detail kebijakan 1291
Versi kebijakan 1292
Dokumen kebijakan JSON 1292
Pelajari selengkapnya 1292
AmazonRoute53AutoNamingFullAccess 1293
Menggunakan kebijakan ini 1293
Detail kebijakan 1293
Versi kebijakan 1293
Dokumen kebijakan JSON 1293
Pelajari selengkapnya 1294
AmazonRoute53AutoNamingReadOnlyAccess 1294
Menggunakan kebijakan ini 1294
Detail kebijakan 1295
Versi kebijakan 1295
Dokumen kebijakan JSON 1295
Pelajari selengkapnya 1295
AmazonRoute53AutoNamingRegistrantAccess 1296
Menggunakan kebijakan ini 1296
Detail kebijakan 1296
Versi kebijakan 1296
Dokumen kebijakan JSON 1296
Pelajari selengkapnya 1297

AmazonRoute53DomainsFullAccess 1297
Menggunakan kebijakan ini 1297
Detail kebijakan 1297
Versi kebijakan 1298
Dokumen kebijakan JSON 1298
Pelajari selengkapnya 1298
AmazonRoute53DomainsReadOnlyAccess 1299
Menggunakan kebijakan ini 1299
Detail kebijakan 1299
Versi kebijakan 1299
Dokumen kebijakan JSON 1299
Pelajari selengkapnya 1300
AmazonRoute53FullAccess 1300
Menggunakan kebijakan ini 1300
Detail kebijakan 1300
Versi kebijakan 1300
Dokumen kebijakan JSON 1301
Pelajari selengkapnya 1302
AmazonRoute53GlobalResolverFullAccess 1302
Menggunakan kebijakan ini 1302
Detail kebijakan 1302
Versi kebijakan 1302
Dokumen kebijakan JSON 1302
Pelajari selengkapnya 1304
AmazonRoute53GlobalResolverReadOnlyAccess 1304
Menggunakan kebijakan ini 1304
Detail kebijakan 1305
Versi kebijakan 1305
Dokumen kebijakan JSON 1305
Pelajari selengkapnya 1306
AmazonRoute53ProfilesFullAccess 1306
Menggunakan kebijakan ini 1306
Detail kebijakan 1306
Versi kebijakan 1306
Dokumen kebijakan JSON 1307
Pelajari selengkapnya 1308

AmazonRoute53ProfilesReadOnlyAccess 1308
Menggunakan kebijakan ini 1308
Detail kebijakan 1308
Versi kebijakan 1308
Dokumen kebijakan JSON 1309
Pelajari selengkapnya 1309
AmazonRoute53ReadOnlyAccess 1309
Menggunakan kebijakan ini 1310
Detail kebijakan 1310
Versi kebijakan 1310
Dokumen kebijakan JSON 1310
Pelajari selengkapnya 1311
AmazonRoute53RecoveryClusterFullAccess 1311
Menggunakan kebijakan ini 1311
Detail kebijakan 1311
Versi kebijakan 1311
Dokumen kebijakan JSON 1311
Pelajari selengkapnya 1312
AmazonRoute53RecoveryClusterReadOnlyAccess 1312
Menggunakan kebijakan ini 1312
Detail kebijakan 1312
Versi kebijakan 1313
Dokumen kebijakan JSON 1313
Pelajari selengkapnya 1313
AmazonRoute53RecoveryControlConfigFullAccess 1313
Menggunakan kebijakan ini 1314
Detail kebijakan 1314
Versi kebijakan 1314
Dokumen kebijakan JSON 1314
Pelajari selengkapnya 1314
AmazonRoute53RecoveryControlConfigReadOnlyAccess 1315
Menggunakan kebijakan ini 1315
Detail kebijakan 1315
Versi kebijakan 1315
Dokumen kebijakan JSON 1315
Pelajari selengkapnya 1316

AmazonRoute53RecoveryReadinessFullAccess 1316
Menggunakan kebijakan ini 1316
Detail kebijakan 1316
Versi kebijakan 1317
Dokumen kebijakan JSON 1317
Pelajari selengkapnya 1317
AmazonRoute53RecoveryReadinessReadOnlyAccess 1317
Menggunakan kebijakan ini 1318
Detail kebijakan 1318
Versi kebijakan 1318
Dokumen kebijakan JSON 1318
Pelajari selengkapnya 1319
AmazonRoute53ResolverFullAccess 1319
Menggunakan kebijakan ini 1319
Detail kebijakan 1319
Versi kebijakan 1320
Dokumen kebijakan JSON 1320
Pelajari selengkapnya 1320
AmazonRoute53ResolverReadOnlyAccess 1321
Menggunakan kebijakan ini 1321
Detail kebijakan 1321
Versi kebijakan 1321
Dokumen kebijakan JSON 1321
Pelajari selengkapnya 1322
AmazonS3ExpressFullAccess 1322
Menggunakan kebijakan ini 1322
Detail kebijakan 1322
Versi kebijakan 1323
Dokumen kebijakan JSON 1323
Pelajari selengkapnya 1323
AmazonS3ExpressReadOnlyAccess 1323
Menggunakan kebijakan ini 1324
Detail kebijakan 1324
Versi kebijakan 1324
Dokumen kebijakan JSON 1324
Pelajari selengkapnya 1325

AmazonS3FilesClientFullAccess 1325
Menggunakan kebijakan ini 1325
Detail kebijakan 1325
Versi kebijakan 1326
Dokumen kebijakan JSON 1326
Pelajari selengkapnya 1326
AmazonS3FilesClientReadOnlyAccess 1326
Menggunakan kebijakan ini 1327
Detail kebijakan 1327
Versi kebijakan 1327
Dokumen kebijakan JSON 1327
Pelajari selengkapnya 1327
AmazonS3FilesClientReadWriteAccess 1328
Menggunakan kebijakan ini 1328
Detail kebijakan 1328
Versi kebijakan 1328
Dokumen kebijakan JSON 1328
Pelajari selengkapnya 1329
AmazonS3FilesCSIDriverPolicy 1329
Menggunakan kebijakan ini 1329
Detail kebijakan 1329
Versi kebijakan 1329
Dokumen kebijakan JSON 1330
Pelajari selengkapnya 1331
AmazonS3FilesFullAccess 1331
Menggunakan kebijakan ini 1331
Detail kebijakan 1332
Versi kebijakan 1332
Dokumen kebijakan JSON 1332
Pelajari selengkapnya 1334
AmazonS3FilesReadOnlyAccess 1334
Menggunakan kebijakan ini 1334
Detail kebijakan 1334
Versi kebijakan 1334
Dokumen kebijakan JSON 1335
Pelajari selengkapnya 1335

AmazonS3FullAccess 1336
Menggunakan kebijakan ini 1336
Detail kebijakan 1336
Versi kebijakan 1336
Dokumen kebijakan JSON 1336
Pelajari selengkapnya 1337
AmazonS3ObjectLambdaExecutionRolePolicy 1337
Menggunakan kebijakan ini 1337
Detail kebijakan 1337
Versi kebijakan 1337
Dokumen kebijakan JSON 1338
Pelajari selengkapnya 1338
AmazonS3OutpostsFullAccess 1338
Menggunakan kebijakan ini 1338
Detail kebijakan 1339
Versi kebijakan 1339
Dokumen kebijakan JSON 1339
Pelajari selengkapnya 1340
AmazonS3OutpostsReadOnlyAccess 1340
Menggunakan kebijakan ini 1340
Detail kebijakan 1340
Versi kebijakan 1341
Dokumen kebijakan JSON 1341
Pelajari selengkapnya 1342
AmazonS3ReadOnlyAccess 1342
Menggunakan kebijakan ini 1342
Detail kebijakan 1342
Versi kebijakan 1343
Dokumen kebijakan JSON 1343
Pelajari selengkapnya 1343
AmazonS3TablesFullAccess 1343
Menggunakan kebijakan ini 1344
Detail kebijakan 1344
Versi kebijakan 1344
Dokumen kebijakan JSON 1344
Pelajari selengkapnya 1345

AmazonS3TablesLakeFormationServiceRole 1345
Menggunakan kebijakan ini 1345
Detail kebijakan 1345
Versi kebijakan 1346
Dokumen kebijakan JSON 1346
Pelajari selengkapnya 1348
AmazonS3TablesReadOnlyAccess 1348
Menggunakan kebijakan ini 1348
Detail kebijakan 1348
Versi kebijakan 1349
Dokumen kebijakan JSON 1349
Pelajari selengkapnya 1349
AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy 1349
Menggunakan kebijakan ini 1350
Detail kebijakan 1350
Versi kebijakan 1350
Dokumen kebijakan JSON 1350
Pelajari selengkapnya 1362
AmazonSageMakerCanvasAIServicesAccess 1362
Menggunakan kebijakan ini 1362
Detail kebijakan 1362
Versi kebijakan 1362
Dokumen kebijakan JSON 1363
Pelajari selengkapnya 1366
AmazonSageMakerCanvasBedrockAccess 1366
Menggunakan kebijakan ini 1366
Detail kebijakan 1366
Versi kebijakan 1366
Dokumen kebijakan JSON 1366
Pelajari selengkapnya 1367
AmazonSageMakerCanvasDataPrepFullAccess 1367
Menggunakan kebijakan ini 1368
Detail kebijakan 1368
Versi kebijakan 1368
Dokumen kebijakan JSON 1368
Pelajari selengkapnya 1377

AmazonSageMakerCanvasDirectDeployAccess 1378
Menggunakan kebijakan ini 1378
Detail kebijakan 1378
Versi kebijakan 1378
Dokumen kebijakan JSON 1378
Pelajari selengkapnya 1379
AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy 1379
Menggunakan kebijakan ini 1380
Detail kebijakan 1380
Versi kebijakan 1380
Dokumen kebijakan JSON 1380
Pelajari selengkapnya 1381
AmazonSageMakerCanvasForecastAccess 1382
Menggunakan kebijakan ini 1382
Detail kebijakan 1382
Versi kebijakan 1382
Dokumen kebijakan JSON 1382
Pelajari selengkapnya 1383
AmazonSageMakerCanvasFullAccess 1383
Menggunakan kebijakan ini 1384
Detail kebijakan 1384
Versi kebijakan 1384
Dokumen kebijakan JSON 1384
Pelajari selengkapnya 1396
AmazonSageMakerCanvasSMDataScienceAssistantAccess 1396
Menggunakan kebijakan ini 1397
Detail kebijakan 1397
Versi kebijakan 1397
Dokumen kebijakan JSON 1397
Pelajari selengkapnya 1398
AmazonSageMakerCapacityReservationServiceRolePolicy 1398
Menggunakan kebijakan ini 1398
Detail kebijakan 1399
Versi kebijakan 1399
Dokumen kebijakan JSON 1399
Pelajari selengkapnya 1400

AmazonSageMakerClusterInstanceRolePolicy 1400
Menggunakan kebijakan ini 1400
Detail kebijakan 1400
Versi kebijakan 1400
Dokumen kebijakan JSON 1400
Pelajari selengkapnya 1402
AmazonSageMakerCoreServiceRolePolicy 1402
Menggunakan kebijakan ini 1402
Detail kebijakan 1403
Versi kebijakan 1403
Dokumen kebijakan JSON 1403
Pelajari selengkapnya 1404
AmazonSageMakerEdgeDeviceFleetPolicy 1404
Menggunakan kebijakan ini 1404
Detail kebijakan 1404
Versi kebijakan 1405
Dokumen kebijakan JSON 1405
Pelajari selengkapnya 1407
AmazonSageMakerFeatureStoreAccess 1407
Menggunakan kebijakan ini 1407
Detail kebijakan 1407
Versi kebijakan 1407
Dokumen kebijakan JSON 1408
Pelajari selengkapnya 1409
AmazonSageMakerFullAccess 1409
Menggunakan kebijakan ini 1409
Detail kebijakan 1409
Versi kebijakan 1409
Dokumen kebijakan JSON 1409
Pelajari selengkapnya 1426
AmazonSageMakerGeospatialExecutionRole 1426
Menggunakan kebijakan ini 1426
Detail kebijakan 1426
Versi kebijakan 1427
Dokumen kebijakan JSON 1427
Pelajari selengkapnya 1428

AmazonSageMakerGeospatialFullAccess 1428
Menggunakan kebijakan ini 1428
Detail kebijakan 1428
Versi kebijakan 1428
Dokumen kebijakan JSON 1429
Pelajari selengkapnya 1429
AmazonSageMakerGroundTruthExecution 1429
Menggunakan kebijakan ini 1430
Detail kebijakan 1430
Versi kebijakan 1430
Dokumen kebijakan JSON 1430
Pelajari selengkapnya 1434
AmazonSageMakerHyperPodGatedModelAccess 1434
Menggunakan kebijakan ini 1434
Detail kebijakan 1434
Versi kebijakan 1434
Dokumen kebijakan JSON 1435
Pelajari selengkapnya 1435
AmazonSageMakerHyperPodInferenceAccess 1435
Menggunakan kebijakan ini 1436
Detail kebijakan 1436
Versi kebijakan 1436
Dokumen kebijakan JSON 1436
Pelajari selengkapnya 1445
AmazonSageMakerHyperPodInferenceGatewayAccess 1445
Menggunakan kebijakan ini 1445
Detail kebijakan 1445
Versi kebijakan 1446
Dokumen kebijakan JSON 1446
Pelajari selengkapnya 1447
AmazonSageMakerHyperPodObservabilityAdminAccess 1447
Menggunakan kebijakan ini 1448
Detail kebijakan 1448
Versi kebijakan 1448
Dokumen kebijakan JSON 1448
Pelajari selengkapnya 1454

AmazonSageMakerHyperPodServiceRolePolicy 1455
Menggunakan kebijakan ini 1455
Detail kebijakan 1455
Versi kebijakan 1455
Dokumen kebijakan JSON 1455
Pelajari selengkapnya 1456
AmazonSageMakerHyperPodTrainingOperatorAccess 1457
Menggunakan kebijakan ini 1457
Detail kebijakan 1457
Versi kebijakan 1457
Dokumen kebijakan JSON 1457
Pelajari selengkapnya 1458
AmazonSageMakerInferenceServiceRolePolicy 1458
Menggunakan kebijakan ini 1458
Detail kebijakan 1458
Versi kebijakan 1459
Dokumen kebijakan JSON 1459
Pelajari selengkapnya 1461
AmazonSageMakerJobFullAccess 1462
Menggunakan kebijakan ini 1462
Detail kebijakan 1462
Versi kebijakan 1462
Dokumen kebijakan JSON 1462
Pelajari selengkapnya 1467
AmazonSageMakerJobRuntimeAccess 1467
Menggunakan kebijakan ini 1467
Detail kebijakan 1467
Versi kebijakan 1468
Dokumen kebijakan JSON 1468
Pelajari selengkapnya 1469
AmazonSageMakerMechanicalTurkAccess 1469
Menggunakan kebijakan ini 1470
Detail kebijakan 1470
Versi kebijakan 1470
Dokumen kebijakan JSON 1470
Pelajari selengkapnya 1470

AmazonSageMakerModelCustomizationCoreAccess 1471
Menggunakan kebijakan ini 1471
Detail kebijakan 1471
Versi kebijakan 1471
Dokumen kebijakan JSON 1471
Pelajari selengkapnya 1483
AmazonSageMakerModelGovernanceUseAccess 1483
Menggunakan kebijakan ini 1483
Detail kebijakan 1484
Versi kebijakan 1484
Dokumen kebijakan JSON 1484
Pelajari selengkapnya 1486
AmazonSageMakerModelRegistryFullAccess 1486
Menggunakan kebijakan ini 1486
Detail kebijakan 1486
Versi kebijakan 1487
Dokumen kebijakan JSON 1487
Pelajari selengkapnya 1490
AmazonSageMakerNotebooksServiceRolePolicy 1491
Menggunakan kebijakan ini 1491
Detail kebijakan 1491
Versi kebijakan 1491
Dokumen kebijakan JSON 1491
Pelajari selengkapnya 1496
AmazonSageMakerPartnerAppsFullAccess 1497
Menggunakan kebijakan ini 1497
Detail kebijakan 1497
Versi kebijakan 1497
Dokumen kebijakan JSON 1497
Pelajari selengkapnya 1498
AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy 1498
Menggunakan kebijakan ini 1498
Detail kebijakan 1499
Versi kebijakan 1499
Dokumen kebijakan JSON 1499
Pelajari selengkapnya 1500

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy 1500
Menggunakan kebijakan ini 1500
Detail kebijakan 1500
Versi kebijakan 1501
Dokumen kebijakan JSON 1501
Pelajari selengkapnya 1504
AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy 1505
Menggunakan kebijakan ini 1505
Detail kebijakan 1505
Versi kebijakan 1505
Dokumen kebijakan JSON 1505
Pelajari selengkapnya 1506
AmazonSageMakerPipelinesIntegrations 1506
Menggunakan kebijakan ini 1506
Detail kebijakan 1506
Versi kebijakan 1507
Dokumen kebijakan JSON 1507
Pelajari selengkapnya 1509
AmazonSageMakerQuickSightVPCPolicy 1509
Menggunakan kebijakan ini 1509
Detail kebijakan 1509
Versi kebijakan 1509
Dokumen kebijakan JSON 1510
Pelajari selengkapnya 1511
AmazonSageMakerReadOnly 1511
Menggunakan kebijakan ini 1511
Detail kebijakan 1512
Versi kebijakan 1512
Dokumen kebijakan JSON 1512
Pelajari selengkapnya 1513
AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy 1513
Menggunakan kebijakan ini 1514
Detail kebijakan 1514
Versi kebijakan 1514
Dokumen kebijakan JSON 1514
Pelajari selengkapnya 1515

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy 1515
Menggunakan kebijakan ini 1515
Detail kebijakan 1515
Versi kebijakan 1516
Dokumen kebijakan JSON 1516
Pelajari selengkapnya 1523
AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy 1523
Menggunakan kebijakan ini 1523
Detail kebijakan 1523
Versi kebijakan 1523
Dokumen kebijakan JSON 1524
Pelajari selengkapnya 1534
AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy 1534
Menggunakan kebijakan ini 1534
Detail kebijakan 1534
Versi kebijakan 1535
Dokumen kebijakan JSON 1535
Pelajari selengkapnya 1538
AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy 1538
Menggunakan kebijakan ini 1538
Detail kebijakan 1538
Versi kebijakan 1538
Dokumen kebijakan JSON 1539
Pelajari selengkapnya 1539
AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy 1539
Menggunakan kebijakan ini 1539
Detail kebijakan 1539
Versi kebijakan 1540
Dokumen kebijakan JSON 1540
Pelajari selengkapnya 1540
AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy 1541
Menggunakan kebijakan ini 1541
Detail kebijakan 1541
Versi kebijakan 1541
Dokumen kebijakan JSON 1541
Pelajari selengkapnya 1543

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy 1544
Menggunakan kebijakan ini 1544
Detail kebijakan 1544
Versi kebijakan 1544
Dokumen kebijakan JSON 1545
Pelajari selengkapnya 1555
AmazonSageMakerSpacesControllerPolicy 1555
Menggunakan kebijakan ini 1555
Detail kebijakan 1555
Versi kebijakan 1555
Dokumen kebijakan JSON 1556
Pelajari selengkapnya 1560
AmazonSageMakerSpacesRouterPolicy 1560
Menggunakan kebijakan ini 1561
Detail kebijakan 1561
Versi kebijakan 1561
Dokumen kebijakan JSON 1561
Pelajari selengkapnya 1562
AmazonSageMakerTrainingPlanCreateAccess 1562
Menggunakan kebijakan ini 1562
Detail kebijakan 1562
Versi kebijakan 1563
Dokumen kebijakan JSON 1563
Pelajari selengkapnya 1564
AmazonSecurityLakeAdministrator 1565
Menggunakan kebijakan ini 1565
Detail kebijakan 1565
Versi kebijakan 1565
Dokumen kebijakan JSON 1565
Pelajari selengkapnya 1576
AmazonSecurityLakeMetastoreManager 1577
Menggunakan kebijakan ini 1577
Detail kebijakan 1577
Versi kebijakan 1577
Dokumen kebijakan JSON 1577
Pelajari selengkapnya 1580

AmazonSecurityLakePermissionsBoundary 1580
Menggunakan kebijakan ini 1580
Detail kebijakan 1580
Versi kebijakan 1580
Dokumen kebijakan JSON 1581
Pelajari selengkapnya 1584
AmazonSESFullAccess 1584
Menggunakan kebijakan ini 1584
Detail kebijakan 1584
Versi kebijakan 1584
Dokumen kebijakan JSON 1585
Pelajari selengkapnya 1585
AmazonSESReadOnlyAccess 1585
Menggunakan kebijakan ini 1585
Detail kebijakan 1585
Versi kebijakan 1586
Dokumen kebijakan JSON 1586
Pelajari selengkapnya 1586
AmazonSESServiceRolePolicy 1586
Menggunakan kebijakan ini 1587
Detail kebijakan 1587
Versi kebijakan 1587
Dokumen kebijakan JSON 1587
Pelajari selengkapnya 1588
AmazonSNSFullAccess 1588
Menggunakan kebijakan ini 1588
Detail kebijakan 1588
Versi kebijakan 1588
Dokumen kebijakan JSON 1588
Pelajari selengkapnya 1589
AmazonSNSReadOnlyAccess 1590
Menggunakan kebijakan ini 1590
Detail kebijakan 1590
Versi kebijakan 1590
Dokumen kebijakan JSON 1590
Pelajari selengkapnya 1591

AmazonSNSRole 1591
Menggunakan kebijakan ini 1592
Detail kebijakan 1592
Versi kebijakan 1592
Dokumen kebijakan JSON 1592
Pelajari selengkapnya 1593
AmazonSQSFullAccess 1593
Menggunakan kebijakan ini 1593
Detail kebijakan 1593
Versi kebijakan 1593
Dokumen kebijakan JSON 1593
Pelajari selengkapnya 1594
AmazonSQSReadOnlyAccess 1594
Menggunakan kebijakan ini 1594
Detail kebijakan 1594
Versi kebijakan 1594
Dokumen kebijakan JSON 1595
Pelajari selengkapnya 1595
AmazonSSMAutomationApproverAccess 1595
Menggunakan kebijakan ini 1596
Detail kebijakan 1596
Versi kebijakan 1596
Dokumen kebijakan JSON 1596
Pelajari selengkapnya 1597
AmazonSSMAutomationRole 1597
Menggunakan kebijakan ini 1597
Detail kebijakan 1597
Versi kebijakan 1597
Dokumen kebijakan JSON 1597
Pelajari selengkapnya 1599
AmazonSSMDirectoryServiceAccess 1599
Menggunakan kebijakan ini 1600
Detail kebijakan 1600
Versi kebijakan 1600
Dokumen kebijakan JSON 1600
Pelajari selengkapnya 1600

AmazonSSMFullAccess 1601
Menggunakan kebijakan ini 1601
Detail kebijakan 1601
Versi kebijakan 1601
Dokumen kebijakan JSON 1601
Pelajari selengkapnya 1603
AmazonSSMMaintenanceWindowRole 1603
Menggunakan kebijakan ini 1603
Detail kebijakan 1603
Versi kebijakan 1603
Dokumen kebijakan JSON 1603
Pelajari selengkapnya 1605
AmazonSSMManagedEC2InstanceDefaultPolicy 1605
Menggunakan kebijakan ini 1605
Detail kebijakan 1605
Versi kebijakan 1606
Dokumen kebijakan JSON 1606
Pelajari selengkapnya 1607
AmazonSSMManagedInstanceCore 1607
Menggunakan kebijakan ini 1607
Detail kebijakan 1607
Versi kebijakan 1608
Dokumen kebijakan JSON 1608
Pelajari selengkapnya 1609
AmazonSSMPatchAssociation 1609
Menggunakan kebijakan ini 1609
Detail kebijakan 1609
Versi kebijakan 1610
Dokumen kebijakan JSON 1610
Pelajari selengkapnya 1611
AmazonSSMReadOnlyAccess 1611
Menggunakan kebijakan ini 1611
Detail kebijakan 1611
Versi kebijakan 1611
Dokumen kebijakan JSON 1611
Pelajari selengkapnya 1612

AmazonSSMServiceRolePolicy 1612
Menggunakan kebijakan ini 1612
Detail kebijakan 1612
Versi kebijakan 1613
Dokumen kebijakan JSON 1613
Pelajari selengkapnya 1618
AmazonSumerianFullAccess 1618
Menggunakan kebijakan ini 1619
Detail kebijakan 1619
Versi kebijakan 1619
Dokumen kebijakan JSON 1619
Pelajari selengkapnya 1619
AmazonTextractFullAccess 1620
Menggunakan kebijakan ini 1620
Detail kebijakan 1620
Versi kebijakan 1620
Dokumen kebijakan JSON 1620
Pelajari selengkapnya 1621
AmazonTextractServiceRole 1621
Menggunakan kebijakan ini 1621
Detail kebijakan 1621
Versi kebijakan 1621
Dokumen kebijakan JSON 1622
Pelajari selengkapnya 1622
AmazonTimestreamConsoleFullAccess 1622
Menggunakan kebijakan ini 1622
Detail kebijakan 1622
Versi kebijakan 1623
Dokumen kebijakan JSON 1623
Pelajari selengkapnya 1626
AmazonTimestreamFullAccess 1626
Menggunakan kebijakan ini 1626
Detail kebijakan 1626
Versi kebijakan 1626
Dokumen kebijakan JSON 1626
Pelajari selengkapnya 1628

AmazonTimestreamInfluxDBFullAccess 1628
Menggunakan kebijakan ini 1628
Detail kebijakan 1628
Versi kebijakan 1628
Dokumen kebijakan JSON 1629
Pelajari selengkapnya 1631
AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess 1631
Menggunakan kebijakan ini 1632
Detail kebijakan 1632
Versi kebijakan 1632
Dokumen kebijakan JSON 1632
Pelajari selengkapnya 1634
AmazonTimestreamInfluxDBServiceRolePolicy 1635
Menggunakan kebijakan ini 1635
Detail kebijakan 1635
Versi kebijakan 1635
Dokumen kebijakan JSON 1635
Pelajari selengkapnya 1639
AmazonTimestreamReadOnlyAccess 1639
Menggunakan kebijakan ini 1639
Detail kebijakan 1639
Versi kebijakan 1639
Dokumen kebijakan JSON 1639
Pelajari selengkapnya 1640
AmazonTranscribeFullAccess 1640
Menggunakan kebijakan ini 1640
Detail kebijakan 1641
Versi kebijakan 1641
Dokumen kebijakan JSON 1641
Pelajari selengkapnya 1642
AmazonTranscribeReadOnlyAccess 1642
Menggunakan kebijakan ini 1642
Detail kebijakan 1642
Versi kebijakan 1642
Dokumen kebijakan JSON 1642
Pelajari selengkapnya 1643

AmazonVerifiedPermissionsFullAccess 1643
Menggunakan kebijakan ini 1643
Detail kebijakan 1643
Versi kebijakan 1644
Dokumen kebijakan JSON 1644
Pelajari selengkapnya 1644
AmazonVerifiedPermissionsReadOnlyAccess 1645
Menggunakan kebijakan ini 1645
Detail kebijakan 1645
Versi kebijakan 1645
Dokumen kebijakan JSON 1645
Pelajari selengkapnya 1646
AmazonVPCCrossAccountNetworkInterfaceOperations 1646
Menggunakan kebijakan ini 1646
Detail kebijakan 1647
Versi kebijakan 1647
Dokumen kebijakan JSON 1647
Pelajari selengkapnya 1648
AmazonVPCFullAccess 1649
Menggunakan kebijakan ini 1649
Detail kebijakan 1649
Versi kebijakan 1649
Dokumen kebijakan JSON 1649
Pelajari selengkapnya 1653
AmazonVPCNetworkAccessAnalyzerFullAccessPolicy 1653
Menggunakan kebijakan ini 1654
Detail kebijakan 1654
Versi kebijakan 1654
Dokumen kebijakan JSON 1654
Pelajari selengkapnya 1658
AmazonVPCReachabilityAnalyzerFullAccessPolicy 1658
Menggunakan kebijakan ini 1658
Detail kebijakan 1658
Versi kebijakan 1658
Dokumen kebijakan JSON 1659
Pelajari selengkapnya 1662

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy 1662
Menggunakan kebijakan ini 1662
Detail kebijakan 1662
Versi kebijakan 1662
Dokumen kebijakan JSON 1663
Pelajari selengkapnya 1663
AmazonVPCReadOnlyAccess 1663
Menggunakan kebijakan ini 1663
Detail kebijakan 1664
Versi kebijakan 1664
Dokumen kebijakan JSON 1664
Pelajari selengkapnya 1665
AmazonWorkDocsFullAccess 1665
Menggunakan kebijakan ini 1666
Detail kebijakan 1666
Versi kebijakan 1666
Dokumen kebijakan JSON 1666
Pelajari selengkapnya 1667
AmazonWorkDocsReadOnlyAccess 1667
Menggunakan kebijakan ini 1667
Detail kebijakan 1667
Versi kebijakan 1667
Dokumen kebijakan JSON 1667
Pelajari selengkapnya 1668
AmazonWorkMailEventsServiceRolePolicy 1668
Menggunakan kebijakan ini 1668
Detail kebijakan 1668
Versi kebijakan 1669
Dokumen kebijakan JSON 1669
Pelajari selengkapnya 1669
AmazonWorkMailFullAccess 1669
Menggunakan kebijakan ini 1669
Detail kebijakan 1670
Versi kebijakan 1670
Dokumen kebijakan JSON 1670
Pelajari selengkapnya 1672

AmazonWorkMailMessageFlowFullAccess 1672
Menggunakan kebijakan ini 1672
Detail kebijakan 1672
Versi kebijakan 1673
Dokumen kebijakan JSON 1673
Pelajari selengkapnya 1673
AmazonWorkMailMessageFlowReadOnlyAccess 1673
Menggunakan kebijakan ini 1674
Detail kebijakan 1674
Versi kebijakan 1674
Dokumen kebijakan JSON 1674
Pelajari selengkapnya 1674
AmazonWorkMailReadOnlyAccess 1675
Menggunakan kebijakan ini 1675
Detail kebijakan 1675
Versi kebijakan 1675
Dokumen kebijakan JSON 1675
Pelajari selengkapnya 1676
AmazonWorkSpacesAdmin 1676
Menggunakan kebijakan ini 1676
Detail kebijakan 1676
Versi kebijakan 1677
Dokumen kebijakan JSON 1677
Pelajari selengkapnya 1678
AmazonWorkSpacesApplicationManagerAdminAccess 1678
Menggunakan kebijakan ini 1678
Detail kebijakan 1678
Versi kebijakan 1679
Dokumen kebijakan JSON 1679
Pelajari selengkapnya 1679
AmazonWorkspacesPCAAccess 1679
Menggunakan kebijakan ini 1680
Detail kebijakan 1680
Versi kebijakan 1680
Dokumen kebijakan JSON 1680
Pelajari selengkapnya 1681

AmazonWorkSpacesPoolServiceAccess 1681
Menggunakan kebijakan ini 1681
Detail kebijakan 1681
Versi kebijakan 1681
Dokumen kebijakan JSON 1682
Pelajari selengkapnya 1683
AmazonWorkSpacesSecureBrowserReadOnly 1683
Menggunakan kebijakan ini 1683
Detail kebijakan 1683
Versi kebijakan 1683
Dokumen kebijakan JSON 1684
Pelajari selengkapnya 1685
AmazonWorkSpacesSelfServiceAccess 1685
Menggunakan kebijakan ini 1685
Detail kebijakan 1685
Versi kebijakan 1685
Dokumen kebijakan JSON 1686
Pelajari selengkapnya 1686
AmazonWorkSpacesServiceAccess 1686
Menggunakan kebijakan ini 1686
Detail kebijakan 1687
Versi kebijakan 1687
Dokumen kebijakan JSON 1687
Pelajari selengkapnya 1687
AmazonWorkSpacesThinClientFullAccess 1688
Menggunakan kebijakan ini 1688
Detail kebijakan 1688
Versi kebijakan 1688
Dokumen kebijakan JSON 1688
Pelajari selengkapnya 1690
AmazonWorkSpacesThinClientMonitoringServiceRolePolicy 1690
Menggunakan kebijakan ini 1690
Detail kebijakan 1690
Versi kebijakan 1690
Dokumen kebijakan JSON 1691
Pelajari selengkapnya 1691

AmazonWorkSpacesThinClientReadOnlyAccess 1691
Menggunakan kebijakan ini 1691
Detail kebijakan 1692
Versi kebijakan 1692
Dokumen kebijakan JSON 1692
Pelajari selengkapnya 1693
AmazonWorkSpacesWebReadOnly 1693
Menggunakan kebijakan ini 1694
Detail kebijakan 1694
Versi kebijakan 1694
Dokumen kebijakan JSON 1694
Pelajari selengkapnya 1695
AmazonWorkSpacesWebServiceRolePolicy 1695
Menggunakan kebijakan ini 1695
Detail kebijakan 1696
Versi kebijakan 1696
Dokumen kebijakan JSON 1696
Pelajari selengkapnya 1698
AmazonZocaloFullAccess 1698
Menggunakan kebijakan ini 1699
Detail kebijakan 1699
Versi kebijakan 1699
Dokumen kebijakan JSON 1699
Pelajari selengkapnya 1700
AmazonZocaloReadOnlyAccess 1700
Menggunakan kebijakan ini 1700
Detail kebijakan 1700
Versi kebijakan 1700
Dokumen kebijakan JSON 1701
Pelajari selengkapnya 1701
AmplifyBackendDeployFullAccess 1701
Menggunakan kebijakan ini 1702
Detail kebijakan 1702
Versi kebijakan 1702
Dokumen kebijakan JSON 1702
Pelajari selengkapnya 1706

AnthropicFullAccess 1707
Menggunakan kebijakan ini 1707
Detail kebijakan 1707
Versi kebijakan 1707
Dokumen kebijakan JSON 1707
Pelajari selengkapnya 1709
AnthropicLimitedAccess 1709
Menggunakan kebijakan ini 1709
Detail kebijakan 1710
Versi kebijakan 1710
Dokumen kebijakan JSON 1710
Pelajari selengkapnya 1712
AnthropicReadOnlyAccess 1712
Menggunakan kebijakan ini 1713
Detail kebijakan 1713
Versi kebijakan 1713
Dokumen kebijakan JSON 1713
Pelajari selengkapnya 1715
AnthropicSelfHostedEnvironmentAccess 1715
Menggunakan kebijakan ini 1715
Detail kebijakan 1715
Versi kebijakan 1715
Dokumen kebijakan JSON 1715
Pelajari selengkapnya 1716
APIGatewayServiceRolePolicy 1716
Menggunakan kebijakan ini 1717
Detail kebijakan 1717
Versi kebijakan 1717
Dokumen kebijakan JSON 1717
Pelajari selengkapnya 1719
AppIntegrationsServiceLinkedRolePolicy 1719
Menggunakan kebijakan ini 1720
Detail kebijakan 1720
Versi kebijakan 1720
Dokumen kebijakan JSON 1720
Pelajari selengkapnya 1722

ApplicationAutoScalingForAmazonAppStreamAccess 1722
Menggunakan kebijakan ini 1722
Detail kebijakan 1722
Versi kebijakan 1722
Dokumen kebijakan JSON 1723
Pelajari selengkapnya 1723
ApplicationDiscoveryServiceContinuousExportServiceRolePolicy 1723
Menggunakan kebijakan ini 1724
Detail kebijakan 1724
Versi kebijakan 1724
Dokumen kebijakan JSON 1724
Pelajari selengkapnya 1726
AppRunnerNetworkingServiceRolePolicy 1726
Menggunakan kebijakan ini 1726
Detail kebijakan 1727
Versi kebijakan 1727
Dokumen kebijakan JSON 1727
Pelajari selengkapnya 1728
AppRunnerServiceRolePolicy 1728
Menggunakan kebijakan ini 1729
Detail kebijakan 1729
Versi kebijakan 1729
Dokumen kebijakan JSON 1729
Pelajari selengkapnya 1730
AppStudioServiceRolePolicy 1730
Menggunakan kebijakan ini 1730
Detail kebijakan 1730
Versi kebijakan 1731
Dokumen kebijakan JSON 1731
Pelajari selengkapnya 1733
AssuranceServiceRolePolicy 1733
Menggunakan kebijakan ini 1733
Detail kebijakan 1733
Versi kebijakan 1734
Dokumen kebijakan JSON 1734
Pelajari selengkapnya 1744

AuroraDsqlServiceLinkedRolePolicy 1745
Menggunakan kebijakan ini 1745
Detail kebijakan 1745
Versi kebijakan 1745
Dokumen kebijakan JSON 1745
Pelajari selengkapnya 1746
AutoScalingConsoleFullAccess 1746
Menggunakan kebijakan ini 1746
Detail kebijakan 1746
Versi kebijakan 1746
Dokumen kebijakan JSON 1747
Pelajari selengkapnya 1748
AutoScalingConsoleReadOnlyAccess 1749
Menggunakan kebijakan ini 1749
Detail kebijakan 1749
Versi kebijakan 1749
Dokumen kebijakan JSON 1749
Pelajari selengkapnya 1750
AutoScalingFullAccess 1750
Menggunakan kebijakan ini 1751
Detail kebijakan 1751
Versi kebijakan 1751
Dokumen kebijakan JSON 1751
Pelajari selengkapnya 1752
AutoScalingNotificationAccessRole 1753
Menggunakan kebijakan ini 1753
Detail kebijakan 1753
Versi kebijakan 1753
Dokumen kebijakan JSON 1753
Pelajari selengkapnya 1754
AutoScalingReadOnlyAccess 1754
Menggunakan kebijakan ini 1754
Detail kebijakan 1754
Versi kebijakan 1754
Dokumen kebijakan JSON 1755
Pelajari selengkapnya 1755

AutoScalingServiceRolePolicy 1755
Menggunakan kebijakan ini 1755
Detail kebijakan 1755
Versi kebijakan 1756
Dokumen kebijakan JSON 1756
Pelajari selengkapnya 1759
AWS-SSM-Automation-DiagnosisBucketPolicy 1759
Menggunakan kebijakan ini 1759
Detail kebijakan 1759
Versi kebijakan 1759
Dokumen kebijakan JSON 1760
Pelajari selengkapnya 1762
AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy 1762
Menggunakan kebijakan ini 1762
Detail kebijakan 1763
Versi kebijakan 1763
Dokumen kebijakan JSON 1763
Pelajari selengkapnya 1765
AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy 1766
Menggunakan kebijakan ini 1766
Detail kebijakan 1766
Versi kebijakan 1766
Dokumen kebijakan JSON 1766
Pelajari selengkapnya 1769
AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy 1769
Menggunakan kebijakan ini 1769
Detail kebijakan 1770
Versi kebijakan 1770
Dokumen kebijakan JSON 1770
Pelajari selengkapnya 1771
AWS-SSM-RemediationAutomation-AdministrationRolePolicy 1771
Menggunakan kebijakan ini 1771
Detail kebijakan 1771
Versi kebijakan 1771
Dokumen kebijakan JSON 1772
Pelajari selengkapnya 1774

AWS-SSM-RemediationAutomation-ExecutionRolePolicy 1774
Menggunakan kebijakan ini 1775
Detail kebijakan 1775
Versi kebijakan 1775
Dokumen kebijakan JSON 1775
Pelajari selengkapnya 1781
AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy 1782
Menggunakan kebijakan ini 1782
Detail kebijakan 1782
Versi kebijakan 1782
Dokumen kebijakan JSON 1782
Pelajari selengkapnya 1783
AWS_ConfigRole 1783
Menggunakan kebijakan ini 1783
Detail kebijakan 1784
Versi kebijakan 1784
Dokumen kebijakan JSON 1784
Pelajari selengkapnya 1843
AWSAccountActivityAccess 1843
Menggunakan kebijakan ini 1843
Detail kebijakan 1843
Versi kebijakan 1843
Dokumen kebijakan JSON 1843
Pelajari selengkapnya 1844
AWSAccountManagementFullAccess 1844
Menggunakan kebijakan ini 1844
Detail kebijakan 1845
Versi kebijakan 1845
Dokumen kebijakan JSON 1845
Pelajari selengkapnya 1845
AWSAccountManagementReadOnlyAccess 1846
Menggunakan kebijakan ini 1846
Detail kebijakan 1846
Versi kebijakan 1846
Dokumen kebijakan JSON 1846
Pelajari selengkapnya 1847

AWSAccountSettingsManagementRole 1847
Menggunakan kebijakan ini 1847
Detail kebijakan 1847
Versi kebijakan 1847
Dokumen kebijakan JSON 1848
Pelajari selengkapnya 1850
AWSAccountUsageReportAccess 1851
Menggunakan kebijakan ini 1851
Detail kebijakan 1851
Versi kebijakan 1851
Dokumen kebijakan JSON 1851
Pelajari selengkapnya 1852
AWSAgentlessDiscoveryService 1852
Menggunakan kebijakan ini 1852
Detail kebijakan 1852
Versi kebijakan 1852
Dokumen kebijakan JSON 1852
Pelajari selengkapnya 1854
AWSAgentRegistryServiceRolePolicy 1854
Menggunakan kebijakan ini 1855
Detail kebijakan 1855
Versi kebijakan 1855
Dokumen kebijakan JSON 1855
Pelajari selengkapnya 1857
AWSAppConfigServiceRolePolicy 1858
Menggunakan kebijakan ini 1858
Detail kebijakan 1858
Versi kebijakan 1858
Dokumen kebijakan JSON 1858
Pelajari selengkapnya 1859
AWSAppFabricFullAccess 1859
Menggunakan kebijakan ini 1859
Detail kebijakan 1859
Versi kebijakan 1859
Dokumen kebijakan JSON 1860
Pelajari selengkapnya 1861

AWSAppFabricReadOnlyAccess 1861
Menggunakan kebijakan ini 1861
Detail kebijakan 1861
Versi kebijakan 1862
Dokumen kebijakan JSON 1862
Pelajari selengkapnya 1862
AWSAppFabricServiceRolePolicy 1863
Menggunakan kebijakan ini 1863
Detail kebijakan 1863
Versi kebijakan 1863
Dokumen kebijakan JSON 1863
Pelajari selengkapnya 1864
AWSApplicationAutoscalingAppStreamFleetPolicy 1865
Menggunakan kebijakan ini 1865
Detail kebijakan 1865
Versi kebijakan 1865
Dokumen kebijakan JSON 1865
Pelajari selengkapnya 1866
AWSApplicationAutoscalingCassandraTablePolicy 1866
Menggunakan kebijakan ini 1866
Detail kebijakan 1866
Versi kebijakan 1866
Dokumen kebijakan JSON 1867
Pelajari selengkapnya 1867
AWSApplicationAutoscalingComprehendEndpointPolicy 1867
Menggunakan kebijakan ini 1868
Detail kebijakan 1868
Versi kebijakan 1868
Dokumen kebijakan JSON 1868
Pelajari selengkapnya 1869
AWSApplicationAutoScalingCustomResourcePolicy 1869
Menggunakan kebijakan ini 1869
Detail kebijakan 1869
Versi kebijakan 1869
Dokumen kebijakan JSON 1870
Pelajari selengkapnya 1870

AWSApplicationAutoscalingDynamoDBTablePolicy 1870
Menggunakan kebijakan ini 1870
Detail kebijakan 1870
Versi kebijakan 1871
Dokumen kebijakan JSON 1871
Pelajari selengkapnya 1871
AWSApplicationAutoscalingEC2SpotFleetRequestPolicy 1872
Menggunakan kebijakan ini 1872
Detail kebijakan 1872
Versi kebijakan 1872
Dokumen kebijakan JSON 1872
Pelajari selengkapnya 1873
AWSApplicationAutoscalingECSServicePolicy 1873
Menggunakan kebijakan ini 1873
Detail kebijakan 1873
Versi kebijakan 1874
Dokumen kebijakan JSON 1874
Pelajari selengkapnya 1874
AWSApplicationAutoscalingElastiCacheRGPolicy 1874
Menggunakan kebijakan ini 1875
Detail kebijakan 1875
Versi kebijakan 1875
Dokumen kebijakan JSON 1875
Pelajari selengkapnya 1876
AWSApplicationAutoscalingEMRInstanceGroupPolicy 1876
Menggunakan kebijakan ini 1877
Detail kebijakan 1877
Versi kebijakan 1877
Dokumen kebijakan JSON 1877
Pelajari selengkapnya 1878
AWSApplicationAutoscalingKafkaClusterPolicy 1878
Menggunakan kebijakan ini 1878
Detail kebijakan 1878
Versi kebijakan 1878
Dokumen kebijakan JSON 1878
Pelajari selengkapnya 1879

AWSApplicationAutoscalingLambdaConcurrencyPolicy 1879
Menggunakan kebijakan ini 1879
Detail kebijakan 1879
Versi kebijakan 1880
Dokumen kebijakan JSON 1880
Pelajari selengkapnya 1880
AWSApplicationAutoscalingNeptuneClusterPolicy 1881
Menggunakan kebijakan ini 1881
Detail kebijakan 1881
Versi kebijakan 1881
Dokumen kebijakan JSON 1881
Pelajari selengkapnya 1883
AWSApplicationAutoscalingRDSClusterPolicy 1883
Menggunakan kebijakan ini 1883
Detail kebijakan 1883
Versi kebijakan 1883
Dokumen kebijakan JSON 1884
Pelajari selengkapnya 1884
AWSApplicationAutoscalingSageMakerEndpointPolicy 1885
Menggunakan kebijakan ini 1885
Detail kebijakan 1885
Versi kebijakan 1885
Dokumen kebijakan JSON 1885
Pelajari selengkapnya 1886
AWSApplicationAutoscalingWorkSpacesPoolPolicy 1886
Menggunakan kebijakan ini 1887
Detail kebijakan 1887
Versi kebijakan 1887
Dokumen kebijakan JSON 1887
Pelajari selengkapnya 1888
AWSApplicationDiscoveryAgentAccess 1889
Menggunakan kebijakan ini 1889
Detail kebijakan 1889
Versi kebijakan 1889
Dokumen kebijakan JSON 1889
Pelajari selengkapnya 1890

AWSApplicationDiscoveryAgentlessCollectorAccess 1890
Menggunakan kebijakan ini 1890
Detail kebijakan 1890
Versi kebijakan 1891
Dokumen kebijakan JSON 1891
Pelajari selengkapnya 1892
AWSApplicationDiscoveryServiceFullAccess 1892
Menggunakan kebijakan ini 1892
Detail kebijakan 1892
Versi kebijakan 1892
Dokumen kebijakan JSON 1893
Pelajari selengkapnya 1894
AWSApplicationMigrationAgentInstallationPolicy 1894
Menggunakan kebijakan ini 1895
Detail kebijakan 1895
Versi kebijakan 1895
Dokumen kebijakan JSON 1895
Pelajari selengkapnya 1896
AWSApplicationMigrationAgentPolicy 1896
Menggunakan kebijakan ini 1896
Detail kebijakan 1897
Versi kebijakan 1897
Dokumen kebijakan JSON 1897
Pelajari selengkapnya 1898
AWSApplicationMigrationAgentPolicy_v2 1898
Menggunakan kebijakan ini 1898
Detail kebijakan 1898
Versi kebijakan 1899
Dokumen kebijakan JSON 1899
Pelajari selengkapnya 1899
AWSApplicationMigrationConversionServerPolicy 1900
Menggunakan kebijakan ini 1900
Detail kebijakan 1900
Versi kebijakan 1900
Dokumen kebijakan JSON 1901
Pelajari selengkapnya 1901

AWSApplicationMigrationEC2Access 1901
Menggunakan kebijakan ini 1901
Detail kebijakan 1902
Versi kebijakan 1902
Dokumen kebijakan JSON 1902
Pelajari selengkapnya 1910
AWSApplicationMigrationFSxProxyPolicy 1910
Menggunakan kebijakan ini 1910
Detail kebijakan 1910
Versi kebijakan 1911
Dokumen kebijakan JSON 1911
Pelajari selengkapnya 1914
AWSApplicationMigrationFSxProxyVPCPolicy 1914
Menggunakan kebijakan ini 1914
Detail kebijakan 1914
Versi kebijakan 1914
Dokumen kebijakan JSON 1915
Pelajari selengkapnya 1919
AWSApplicationMigrationFullAccess 1919
Menggunakan kebijakan ini 1919
Detail kebijakan 1919
Versi kebijakan 1920
Dokumen kebijakan JSON 1920
Pelajari selengkapnya 1928
AWSApplicationMigrationMGHAccess 1928
Menggunakan kebijakan ini 1929
Detail kebijakan 1929
Versi kebijakan 1929
Dokumen kebijakan JSON 1929
Pelajari selengkapnya 1930
AWSApplicationMigrationNetworkMigrationCustomResource 1930
Menggunakan kebijakan ini 1930
Detail kebijakan 1930
Versi kebijakan 1930
Dokumen kebijakan JSON 1931
Pelajari selengkapnya 1931

AWSApplicationMigrationNetworkMigrationMultiAccount 1931
Menggunakan kebijakan ini 1932
Detail kebijakan 1932
Versi kebijakan 1932
Dokumen kebijakan JSON 1932
Pelajari selengkapnya 1957
AWSApplicationMigrationReadOnlyAccess 1958
Menggunakan kebijakan ini 1958
Detail kebijakan 1958
Versi kebijakan 1958
Dokumen kebijakan JSON 1958
Pelajari selengkapnya 1960
AWSApplicationMigrationReplicationServerPolicy 1960
Menggunakan kebijakan ini 1960
Detail kebijakan 1960
Versi kebijakan 1961
Dokumen kebijakan JSON 1961
Pelajari selengkapnya 1962
AWSApplicationMigrationServiceEc2InstancePolicy 1963
Menggunakan kebijakan ini 1963
Detail kebijakan 1963
Versi kebijakan 1963
Dokumen kebijakan JSON 1963
Pelajari selengkapnya 1964
AWSApplicationMigrationServiceRolePolicy 1965
Menggunakan kebijakan ini 1965
Detail kebijakan 1965
Versi kebijakan 1965
Dokumen kebijakan JSON 1965
Pelajari selengkapnya 1973
AWSApplicationMigrationSSMAccess 1973
Menggunakan kebijakan ini 1973
Detail kebijakan 1973
Versi kebijakan 1973
Dokumen kebijakan JSON 1974
Pelajari selengkapnya 1975

AWSApplicationMigrationVCenterClientPolicy 1976
Menggunakan kebijakan ini 1976
Detail kebijakan 1976
Versi kebijakan 1976
Dokumen kebijakan JSON 1976
Pelajari selengkapnya 1977
AWSAppMeshEnvoyAccess 1977
Menggunakan kebijakan ini 1977
Detail kebijakan 1978
Versi kebijakan 1978
Dokumen kebijakan JSON 1978
Pelajari selengkapnya 1978
AWSAppMeshFullAccess 1979
Menggunakan kebijakan ini 1979
Detail kebijakan 1979
Versi kebijakan 1979
Dokumen kebijakan JSON 1979
Pelajari selengkapnya 1981
AWSAppMeshPreviewEnvoyAccess 1981
Menggunakan kebijakan ini 1981
Detail kebijakan 1981
Versi kebijakan 1981
Dokumen kebijakan JSON 1981
Pelajari selengkapnya 1982
AWSAppMeshPreviewServiceRolePolicy 1982
Menggunakan kebijakan ini 1982
Detail kebijakan 1982
Versi kebijakan 1983
Dokumen kebijakan JSON 1983
Pelajari selengkapnya 1983
AWSAppMeshReadOnly 1983
Menggunakan kebijakan ini 1984
Detail kebijakan 1984
Versi kebijakan 1984
Dokumen kebijakan JSON 1984
Pelajari selengkapnya 1985

AWSAppMeshServiceRolePolicy 1985
Menggunakan kebijakan ini 1986
Detail kebijakan 1986
Versi kebijakan 1986
Dokumen kebijakan JSON 1986
Pelajari selengkapnya 1987
AWSAppRunnerFullAccess 1987
Menggunakan kebijakan ini 1987
Detail kebijakan 1987
Versi kebijakan 1987
Dokumen kebijakan JSON 1987
Pelajari selengkapnya 1988
AWSAppRunnerReadOnlyAccess 1989
Menggunakan kebijakan ini 1989
Detail kebijakan 1989
Versi kebijakan 1989
Dokumen kebijakan JSON 1989
Pelajari selengkapnya 1990
AWSAppRunnerServicePolicyForECRAccess 1990
Menggunakan kebijakan ini 1990
Detail kebijakan 1990
Versi kebijakan 1990
Dokumen kebijakan JSON 1991
Pelajari selengkapnya 1991
AWSAppSyncAdministrator 1991
Menggunakan kebijakan ini 1991
Detail kebijakan 1992
Versi kebijakan 1992
Dokumen kebijakan JSON 1992
Pelajari selengkapnya 1993
AWSAppSyncInvokeFullAccess 1993
Menggunakan kebijakan ini 1993
Detail kebijakan 1994
Versi kebijakan 1994
Dokumen kebijakan JSON 1994
Pelajari selengkapnya 1994

AWSAppSyncPushToCloudWatchLogs 1995
Menggunakan kebijakan ini 1995
Detail kebijakan 1995
Versi kebijakan 1995
Dokumen kebijakan JSON 1995
Pelajari selengkapnya 1996
AWSAppSyncSchemaAuthor 1996
Menggunakan kebijakan ini 1996
Detail kebijakan 1996
Versi kebijakan 1996
Dokumen kebijakan JSON 1997
Pelajari selengkapnya 1998
AWSAppSyncServiceRolePolicy 1998
Menggunakan kebijakan ini 1998
Detail kebijakan 1998
Versi kebijakan 1998
Dokumen kebijakan JSON 1998
Pelajari selengkapnya 1999
AWSArtifactAccountSync 1999
Menggunakan kebijakan ini 1999
Detail kebijakan 1999
Versi kebijakan 2000
Dokumen kebijakan JSON 2000
Pelajari selengkapnya 2000
AWSArtifactAgreementsFullAccess 2000
Menggunakan kebijakan ini 2001
Detail kebijakan 2001
Versi kebijakan 2001
Dokumen kebijakan JSON 2001
Pelajari selengkapnya 2003
AWSArtifactAgreementsReadOnlyAccess 2003
Menggunakan kebijakan ini 2004
Detail kebijakan 2004
Versi kebijakan 2004
Dokumen kebijakan JSON 2004
Pelajari selengkapnya 2005

AWSArtifactComplianceInquiriesFullAccess 2005
Menggunakan kebijakan ini 2005
Detail kebijakan 2006
Versi kebijakan 2006
Dokumen kebijakan JSON 2006
Pelajari selengkapnya 2007
AWSArtifactComplianceInquiriesReadOnlyAccess 2007
Menggunakan kebijakan ini 2007
Detail kebijakan 2008
Versi kebijakan 2008
Dokumen kebijakan JSON 2008
Pelajari selengkapnya 2009
AWSArtifactReportsReadOnlyAccess 2009
Menggunakan kebijakan ini 2009
Detail kebijakan 2009
Versi kebijakan 2009
Dokumen kebijakan JSON 2009
Pelajari selengkapnya 2010
AWSArtifactServiceRolePolicy 2010
Menggunakan kebijakan ini 2010
Detail kebijakan 2010
Versi kebijakan 2011
Dokumen kebijakan JSON 2011
Pelajari selengkapnya 2011
AWSAuditManagerAdministratorAccess 2011
Menggunakan kebijakan ini 2012
Detail kebijakan 2012
Versi kebijakan 2012
Dokumen kebijakan JSON 2012
Pelajari selengkapnya 2016
AWSAuditManagerServiceRolePolicy 2016
Menggunakan kebijakan ini 2016
Detail kebijakan 2017
Versi kebijakan 2017
Dokumen kebijakan JSON 2017
Pelajari selengkapnya 2024

AWSAutoScalingPlansEC2AutoScalingPolicy 2024
Menggunakan kebijakan ini 2024
Detail kebijakan 2024
Versi kebijakan 2024
Dokumen kebijakan JSON 2025
Pelajari selengkapnya 2025
AWSBackupAccessPointOperatorAccess 2025
Menggunakan kebijakan ini 2025
Detail kebijakan 2026
Versi kebijakan 2026
Dokumen kebijakan JSON 2026
Pelajari selengkapnya 2027
AWSBackupAuditAccess 2028
Menggunakan kebijakan ini 2028
Detail kebijakan 2028
Versi kebijakan 2028
Dokumen kebijakan JSON 2029
Pelajari selengkapnya 2030
AWSBackupDataTransferAccess 2030
Menggunakan kebijakan ini 2030
Detail kebijakan 2030
Versi kebijakan 2031
Dokumen kebijakan JSON 2031
Pelajari selengkapnya 2031
AWSBackupFullAccess 2032
Menggunakan kebijakan ini 2032
Detail kebijakan 2032
Versi kebijakan 2032
Dokumen kebijakan JSON 2032
Pelajari selengkapnya 2044
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync 2044
Menggunakan kebijakan ini 2044
Detail kebijakan 2044
Versi kebijakan 2045
Dokumen kebijakan JSON 2045
Pelajari selengkapnya 2046

AWSBackupGuardDutyRolePolicyForScans 2046
Menggunakan kebijakan ini 2046
Detail kebijakan 2046
Versi kebijakan 2046
Dokumen kebijakan JSON 2046
Pelajari selengkapnya 2050
AWSBackupOperatorAccess 2051
Menggunakan kebijakan ini 2051
Detail kebijakan 2051
Versi kebijakan 2051
Dokumen kebijakan JSON 2051
Pelajari selengkapnya 2060
AWSBackupOrganizationAdminAccess 2061
Menggunakan kebijakan ini 2061
Detail kebijakan 2061
Versi kebijakan 2061
Dokumen kebijakan JSON 2061
Pelajari selengkapnya 2063
AWSBackupRestoreAccessForSAPHANA 2063
Menggunakan kebijakan ini 2063
Detail kebijakan 2064
Versi kebijakan 2064
Dokumen kebijakan JSON 2064
Pelajari selengkapnya 2065
AWSBackupSearchOperatorAccess 2065
Menggunakan kebijakan ini 2065
Detail kebijakan 2065
Versi kebijakan 2066
Dokumen kebijakan JSON 2066
Pelajari selengkapnya 2067
AWSBackupServiceLinkedRolePolicyForBackup 2068
Menggunakan kebijakan ini 2068
Detail kebijakan 2068
Versi kebijakan 2068
Dokumen kebijakan JSON 2068
Pelajari selengkapnya 2078

AWSBackupServiceLinkedRolePolicyForBackupTest 2079
Menggunakan kebijakan ini 2079
Detail kebijakan 2079
Versi kebijakan 2079
Dokumen kebijakan JSON 2079
Pelajari selengkapnya 2080
AWSBackupServiceRolePolicyForBackup 2080
Menggunakan kebijakan ini 2080
Detail kebijakan 2080
Versi kebijakan 2081
Dokumen kebijakan JSON 2081
Pelajari selengkapnya 2095
AWSBackupServiceRolePolicyForIndexing 2096
Menggunakan kebijakan ini 2096
Detail kebijakan 2096
Versi kebijakan 2096
Dokumen kebijakan JSON 2096
Pelajari selengkapnya 2097
AWSBackupServiceRolePolicyForItemRestores 2098
Menggunakan kebijakan ini 2098
Detail kebijakan 2098
Versi kebijakan 2098
Dokumen kebijakan JSON 2098
Pelajari selengkapnya 2100
AWSBackupServiceRolePolicyForRestores 2100
Menggunakan kebijakan ini 2101
Detail kebijakan 2101
Versi kebijakan 2101
Dokumen kebijakan JSON 2101
Pelajari selengkapnya 2115
AWSBackupServiceRolePolicyForS3Backup 2115
Menggunakan kebijakan ini 2115
Detail kebijakan 2115
Versi kebijakan 2116
Dokumen kebijakan JSON 2116
Pelajari selengkapnya 2118

AWSBackupServiceRolePolicyForS3Restore 2119
Menggunakan kebijakan ini 2119
Detail kebijakan 2119
Versi kebijakan 2119
Dokumen kebijakan JSON 2119
Pelajari selengkapnya 2121
AWSBackupServiceRolePolicyForScans 2121
Menggunakan kebijakan ini 2121
Detail kebijakan 2121
Versi kebijakan 2121
Dokumen kebijakan JSON 2122
Pelajari selengkapnya 2123
AWSBatchFullAccess 2123
Menggunakan kebijakan ini 2123
Detail kebijakan 2123
Versi kebijakan 2123
Dokumen kebijakan JSON 2123
Pelajari selengkapnya 2125
AWSBatchServiceEventTargetRole 2125
Menggunakan kebijakan ini 2125
Detail kebijakan 2125
Versi kebijakan 2126
Dokumen kebijakan JSON 2126
Pelajari selengkapnya 2126
AWSBatchServiceRole 2126
Menggunakan kebijakan ini 2127
Detail kebijakan 2127
Versi kebijakan 2127
Dokumen kebijakan JSON 2127
Pelajari selengkapnya 2130
AWSBatchServiceRolePolicyForSageMaker 2130
Menggunakan kebijakan ini 2131
Detail kebijakan 2131
Versi kebijakan 2131
Dokumen kebijakan JSON 2131
Pelajari selengkapnya 2133

AWSBCMDataExportsServiceRolePolicy 2133
Menggunakan kebijakan ini 2133
Detail kebijakan 2133
Versi kebijakan 2133
Dokumen kebijakan JSON 2133
Pelajari selengkapnya 2134
AWSBedrockAgentCoreGatewayNetworkServiceRolePolicy 2134
Menggunakan kebijakan ini 2134
Detail kebijakan 2134
Versi kebijakan 2135
Dokumen kebijakan JSON 2135
Pelajari selengkapnya 2136
AWSBedrockAgentCoreIdentityNetworkServiceRolePolicy 2137
Menggunakan kebijakan ini 2137
Detail kebijakan 2137
Versi kebijakan 2137
Dokumen kebijakan JSON 2137
Pelajari selengkapnya 2139
AWSBedrockAgentCoreRuntimeInstancesServiceRolePolicy 2139
Menggunakan kebijakan ini 2139
Detail kebijakan 2139
Versi kebijakan 2140
Dokumen kebijakan JSON 2140
Pelajari selengkapnya 2142
AWSBillingConductorFullAccess 2143
Menggunakan kebijakan ini 2143
Detail kebijakan 2143
Versi kebijakan 2143
Dokumen kebijakan JSON 2143
Pelajari selengkapnya 2144
AWSBillingConductorReadOnlyAccess 2144
Menggunakan kebijakan ini 2144
Detail kebijakan 2144
Versi kebijakan 2145
Dokumen kebijakan JSON 2145
Pelajari selengkapnya 2145

AWSBillingConductorRolePolicy 2146
Menggunakan kebijakan ini 2146
Detail kebijakan 2146
Versi kebijakan 2146
Dokumen kebijakan JSON 2146
Pelajari selengkapnya 2147
AWSBillingReadOnlyAccess 2147
Menggunakan kebijakan ini 2147
Detail kebijakan 2147
Versi kebijakan 2148
Dokumen kebijakan JSON 2148
Pelajari selengkapnya 2150
AWSBillingServiceRolePolicy 2150
Menggunakan kebijakan ini 2150
Detail kebijakan 2150
Versi kebijakan 2151
Dokumen kebijakan JSON 2151
Pelajari selengkapnya 2151
AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM 2151
Menggunakan kebijakan ini 2152
Detail kebijakan 2152
Versi kebijakan 2152
Dokumen kebijakan JSON 2152
Pelajari selengkapnya 2153
AWSBudgetsActionsWithAWSResourceControlAccess 2153
Menggunakan kebijakan ini 2154
Detail kebijakan 2154
Versi kebijakan 2154
Dokumen kebijakan JSON 2154
Pelajari selengkapnya 2155
AWSBudgetsReadOnlyAccess 2156
Menggunakan kebijakan ini 2156
Detail kebijakan 2156
Versi kebijakan 2156
Dokumen kebijakan JSON 2156
Pelajari selengkapnya 2157

AWSBudgetsSpendLimitMemberRolePolicy 2157
Menggunakan kebijakan ini 2157
Detail kebijakan 2157
Versi kebijakan 2157
Dokumen kebijakan JSON 2158
Pelajari selengkapnya 2163
AWSBugBustFullAccess 2164
Menggunakan kebijakan ini 2164
Detail kebijakan 2164
Versi kebijakan 2164
Dokumen kebijakan JSON 2164
Pelajari selengkapnya 2165
AWSBugBustPlayerAccess 2166
Menggunakan kebijakan ini 2166
Detail kebijakan 2166
Versi kebijakan 2166
Dokumen kebijakan JSON 2166
Pelajari selengkapnya 2167
AWSBugBustServiceRolePolicy 2167
Menggunakan kebijakan ini 2168
Detail kebijakan 2168
Versi kebijakan 2168
Dokumen kebijakan JSON 2168
Pelajari selengkapnya 2169
AWSCertificateManagerFullAccess 2169
Menggunakan kebijakan ini 2169
Detail kebijakan 2169
Versi kebijakan 2169
Dokumen kebijakan JSON 2169
Pelajari selengkapnya 2170
AWSCertificateManagerPrivateCAAuditor 2170
Menggunakan kebijakan ini 2171
Detail kebijakan 2171
Versi kebijakan 2171
Dokumen kebijakan JSON 2171
Pelajari selengkapnya 2172

AWSCertificateManagerPrivateCAFullAccess 2172
Menggunakan kebijakan ini 2172
Detail kebijakan 2172
Versi kebijakan 2173
Dokumen kebijakan JSON 2173
Pelajari selengkapnya 2173
AWSCertificateManagerPrivateCAPrivilegedUser 2173
Menggunakan kebijakan ini 2174
Detail kebijakan 2174
Versi kebijakan 2174
Dokumen kebijakan JSON 2174
Pelajari selengkapnya 2175
AWSCertificateManagerPrivateCAReadOnly 2176
Menggunakan kebijakan ini 2176
Detail kebijakan 2176
Versi kebijakan 2176
Dokumen kebijakan JSON 2176
Pelajari selengkapnya 2177
AWSCertificateManagerPrivateCAUser 2177
Menggunakan kebijakan ini 2177
Detail kebijakan 2177
Versi kebijakan 2177
Dokumen kebijakan JSON 2178
Pelajari selengkapnya 2179
AWSCertificateManagerReadOnly 2179
Menggunakan kebijakan ini 2179
Detail kebijakan 2179
Versi kebijakan 2180
Dokumen kebijakan JSON 2180
Pelajari selengkapnya 2180
AWSChatbotServiceLinkedRolePolicy 2181
Menggunakan kebijakan ini 2181
Detail kebijakan 2181
Versi kebijakan 2181
Dokumen kebijakan JSON 2181
Pelajari selengkapnya 2182

AWSCleanRoomsFullAccess 2182
Menggunakan kebijakan ini 2182
Detail kebijakan 2182
Versi kebijakan 2183
Dokumen kebijakan JSON 2183
Pelajari selengkapnya 2187
AWSCleanRoomsFullAccessNoQuerying 2187
Menggunakan kebijakan ini 2188
Detail kebijakan 2188
Versi kebijakan 2188
Dokumen kebijakan JSON 2188
Pelajari selengkapnya 2193
AWSCleanRoomsMLFullAccess 2193
Menggunakan kebijakan ini 2193
Detail kebijakan 2193
Versi kebijakan 2194
Dokumen kebijakan JSON 2194
Pelajari selengkapnya 2198
AWSCleanRoomsMLReadOnlyAccess 2198
Menggunakan kebijakan ini 2198
Detail kebijakan 2198
Versi kebijakan 2198
Dokumen kebijakan JSON 2199
Pelajari selengkapnya 2200
AWSCleanRoomsReadOnlyAccess 2200
Menggunakan kebijakan ini 2200
Detail kebijakan 2200
Versi kebijakan 2200
Dokumen kebijakan JSON 2201
Pelajari selengkapnya 2202
AWSCleanRoomsServiceRolePolicy 2202
Menggunakan kebijakan ini 2202
Detail kebijakan 2202
Versi kebijakan 2203
Dokumen kebijakan JSON 2203
Pelajari selengkapnya 2203

AWSCloud9Administrator 2203
Menggunakan kebijakan ini 2204
Detail kebijakan 2204
Versi kebijakan 2204
Dokumen kebijakan JSON 2204
Pelajari selengkapnya 2206
AWSCloud9EnvironmentMember 2206
Menggunakan kebijakan ini 2206
Detail kebijakan 2206
Versi kebijakan 2206
Dokumen kebijakan JSON 2207
Pelajari selengkapnya 2208
AWSCloud9ServiceRolePolicy 2208
Menggunakan kebijakan ini 2209
Detail kebijakan 2209
Versi kebijakan 2209
Dokumen kebijakan JSON 2209
Pelajari selengkapnya 2212
AWSCloud9SSMInstanceProfile 2212
Menggunakan kebijakan ini 2212
Detail kebijakan 2212
Versi kebijakan 2212
Dokumen kebijakan JSON 2212
Pelajari selengkapnya 2213
AWSCloud9User 2213
Menggunakan kebijakan ini 2213
Detail kebijakan 2213
Versi kebijakan 2214
Dokumen kebijakan JSON 2214
Pelajari selengkapnya 2216
AWSCloudFormationFullAccess 2217
Menggunakan kebijakan ini 2217
Detail kebijakan 2217
Versi kebijakan 2217
Dokumen kebijakan JSON 2217
Pelajari selengkapnya 2218

AWSCloudFormationReadOnlyAccess 2218
Menggunakan kebijakan ini 2218
Detail kebijakan 2218
Versi kebijakan 2218
Dokumen kebijakan JSON 2218
Pelajari selengkapnya 2219
AWSCloudFrontLogger 2219
Menggunakan kebijakan ini 2219
Detail kebijakan 2219
Versi kebijakan 2220
Dokumen kebijakan JSON 2220
Pelajari selengkapnya 2220
AWSCloudFrontVPCOriginServiceRolePolicy 2220
Menggunakan kebijakan ini 2221
Detail kebijakan 2221
Versi kebijakan 2221
Dokumen kebijakan JSON 2221
Pelajari selengkapnya 2224
AWSCloudHSMFullAccess 2224
Menggunakan kebijakan ini 2224
Detail kebijakan 2224
Versi kebijakan 2224
Dokumen kebijakan JSON 2225
Pelajari selengkapnya 2225
AWSCloudHSMReadOnlyAccess 2225
Menggunakan kebijakan ini 2225
Detail kebijakan 2225
Versi kebijakan 2226
Dokumen kebijakan JSON 2226
Pelajari selengkapnya 2226
AWSCloudHSMRole 2226
Menggunakan kebijakan ini 2227
Detail kebijakan 2227
Versi kebijakan 2227
Dokumen kebijakan JSON 2227
Pelajari selengkapnya 2228

AWSCloudMapDiscoverInstanceAccess 2228
Menggunakan kebijakan ini 2228
Detail kebijakan 2228
Versi kebijakan 2228
Dokumen kebijakan JSON 2229
Pelajari selengkapnya 2229
AWSCloudMapFullAccess 2229
Menggunakan kebijakan ini 2229
Detail kebijakan 2229
Versi kebijakan 2230
Dokumen kebijakan JSON 2230
Pelajari selengkapnya 2231
AWSCloudMapReadOnlyAccess 2231
Menggunakan kebijakan ini 2231
Detail kebijakan 2231
Versi kebijakan 2231
Dokumen kebijakan JSON 2231
Pelajari selengkapnya 2232
AWSCloudMapRegisterInstanceAccess 2232
Menggunakan kebijakan ini 2232
Detail kebijakan 2232
Versi kebijakan 2233
Dokumen kebijakan JSON 2233
Pelajari selengkapnya 2233
AWSCloudShellFullAccess 2234
Menggunakan kebijakan ini 2234
Detail kebijakan 2234
Versi kebijakan 2234
Dokumen kebijakan JSON 2234
Pelajari selengkapnya 2235
AWSCloudTrail_FullAccess 2235
Menggunakan kebijakan ini 2235
Detail kebijakan 2235
Versi kebijakan 2235
Dokumen kebijakan JSON 2236
Pelajari selengkapnya 2238

AWSCloudTrail_ReadOnlyAccess 2238
Menggunakan kebijakan ini 2238
Detail kebijakan 2238
Versi kebijakan 2239
Dokumen kebijakan JSON 2239
Pelajari selengkapnya 2239
AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy 2240
Menggunakan kebijakan ini 2240
Detail kebijakan 2240
Versi kebijakan 2240
Dokumen kebijakan JSON 2240
Pelajari selengkapnya 2241
AWSCloudWatchOmniServiceRolePolicy 2241
Menggunakan kebijakan ini 2241
Detail kebijakan 2241
Versi kebijakan 2241
Dokumen kebijakan JSON 2242
Pelajari selengkapnya 2245
AWSCodeArtifactAdminAccess 2246
Menggunakan kebijakan ini 2246
Detail kebijakan 2246
Versi kebijakan 2246
Dokumen kebijakan JSON 2246
Pelajari selengkapnya 2247
AWSCodeArtifactReadOnlyAccess 2247
Menggunakan kebijakan ini 2247
Detail kebijakan 2247
Versi kebijakan 2247
Dokumen kebijakan JSON 2248
Pelajari selengkapnya 2248
AWSCodeBuildAdminAccess 2249
Menggunakan kebijakan ini 2249
Detail kebijakan 2249
Versi kebijakan 2249
Dokumen kebijakan JSON 2249
Pelajari selengkapnya 2253

AWSCodeBuildDeveloperAccess 2253
Menggunakan kebijakan ini 2253
Detail kebijakan 2253
Versi kebijakan 2253
Dokumen kebijakan JSON 2254
Pelajari selengkapnya 2256
AWSCodeBuildReadOnlyAccess 2257
Menggunakan kebijakan ini 2257
Detail kebijakan 2257
Versi kebijakan 2257
Dokumen kebijakan JSON 2257
Pelajari selengkapnya 2259
AWSCodeCommitFullAccess 2259
Menggunakan kebijakan ini 2259
Detail kebijakan 2259
Versi kebijakan 2259
Dokumen kebijakan JSON 2260
Pelajari selengkapnya 2264
AWSCodeCommitPowerUser 2264
Menggunakan kebijakan ini 2265
Detail kebijakan 2265
Versi kebijakan 2265
Dokumen kebijakan JSON 2265
Pelajari selengkapnya 2270
AWSCodeCommitReadOnly 2270
Menggunakan kebijakan ini 2270
Detail kebijakan 2270
Versi kebijakan 2271
Dokumen kebijakan JSON 2271
Pelajari selengkapnya 2273
AWSCodeDeployDeployerAccess 2274
Menggunakan kebijakan ini 2274
Detail kebijakan 2274
Versi kebijakan 2274
Dokumen kebijakan JSON 2274
Pelajari selengkapnya 2276

AWSCodeDeployFullAccess 2276
Menggunakan kebijakan ini 2276
Detail kebijakan 2276
Versi kebijakan 2276
Dokumen kebijakan JSON 2277
Pelajari selengkapnya 2278
AWSCodeDeployReadOnlyAccess 2278
Menggunakan kebijakan ini 2278
Detail kebijakan 2279
Versi kebijakan 2279
Dokumen kebijakan JSON 2279
Pelajari selengkapnya 2280
AWSCodeDeployRole 2280
Menggunakan kebijakan ini 2280
Detail kebijakan 2280
Versi kebijakan 2281
Dokumen kebijakan JSON 2281
Pelajari selengkapnya 2282
AWSCodeDeployRoleForCloudFormation 2282
Menggunakan kebijakan ini 2283
Detail kebijakan 2283
Versi kebijakan 2283
Dokumen kebijakan JSON 2283
Pelajari selengkapnya 2283
AWSCodeDeployRoleForECS 2284
Menggunakan kebijakan ini 2284
Detail kebijakan 2284
Versi kebijakan 2284
Dokumen kebijakan JSON 2284
Pelajari selengkapnya 2285
AWSCodeDeployRoleForECSLimited 2286
Menggunakan kebijakan ini 2286
Detail kebijakan 2286
Versi kebijakan 2286
Dokumen kebijakan JSON 2286
Pelajari selengkapnya 2288

AWSCodeDeployRoleForLambda 2288
Menggunakan kebijakan ini 2288
Detail kebijakan 2288
Versi kebijakan 2289
Dokumen kebijakan JSON 2289
Pelajari selengkapnya 2290
AWSCodeDeployRoleForLambdaLimited 2290
Menggunakan kebijakan ini 2290
Detail kebijakan 2290
Versi kebijakan 2291
Dokumen kebijakan JSON 2291
Pelajari selengkapnya 2292
AWSCodePipeline_FullAccess 2292
Menggunakan kebijakan ini 2292
Detail kebijakan 2292
Versi kebijakan 2293
Dokumen kebijakan JSON 2293
Pelajari selengkapnya 2297
AWSCodePipeline_ReadOnlyAccess 2297
Menggunakan kebijakan ini 2297
Detail kebijakan 2297
Versi kebijakan 2297
Dokumen kebijakan JSON 2297
Pelajari selengkapnya 2299
AWSCodePipelineApproverAccess 2299
Menggunakan kebijakan ini 2299
Detail kebijakan 2299
Versi kebijakan 2299
Dokumen kebijakan JSON 2299
Pelajari selengkapnya 2300
AWSCodePipelineCustomActionAccess 2300
Menggunakan kebijakan ini 2300
Detail kebijakan 2300
Versi kebijakan 2301
Dokumen kebijakan JSON 2301
Pelajari selengkapnya 2301

AWSCodeStarFullAccess 2302
Menggunakan kebijakan ini 2302
Detail kebijakan 2302
Versi kebijakan 2302
Dokumen kebijakan JSON 2302
Pelajari selengkapnya 2303
AWSCodeStarNotificationsServiceRolePolicy 2303
Menggunakan kebijakan ini 2303
Detail kebijakan 2303
Versi kebijakan 2304
Dokumen kebijakan JSON 2304
Pelajari selengkapnya 2305
AWSCodeStarServiceRole 2305
Menggunakan kebijakan ini 2305
Detail kebijakan 2305
Versi kebijakan 2306
Dokumen kebijakan JSON 2306
Pelajari selengkapnya 2311
AWSCompromisedKeyQuarantine 2311
Menggunakan kebijakan ini 2312
Detail kebijakan 2312
Versi kebijakan 2312
Dokumen kebijakan JSON 2312
Pelajari selengkapnya 2313
AWSCompromisedKeyQuarantineV2 2313
Menggunakan kebijakan ini 2314
Detail kebijakan 2314
Versi kebijakan 2314
Dokumen kebijakan JSON 2314
Pelajari selengkapnya 2317
AWSCompromisedKeyQuarantineV3 2317
Menggunakan kebijakan ini 2317
Detail kebijakan 2317
Versi kebijakan 2317
Dokumen kebijakan JSON 2318
Pelajari selengkapnya 2320

AWSConfigMultiAccountSetupPolicy 2321
Menggunakan kebijakan ini 2321
Detail kebijakan 2321
Versi kebijakan 2321
Dokumen kebijakan JSON 2321
Pelajari selengkapnya 2323
AWSConfigRemediationServiceRolePolicy 2323
Menggunakan kebijakan ini 2324
Detail kebijakan 2324
Versi kebijakan 2324
Dokumen kebijakan JSON 2324
Pelajari selengkapnya 2325
AWSConfigRoleForOrganizations 2325
Menggunakan kebijakan ini 2325
Detail kebijakan 2325
Versi kebijakan 2325
Dokumen kebijakan JSON 2326
Pelajari selengkapnya 2326
AWSConfigRulesExecutionRole 2326
Menggunakan kebijakan ini 2326
Detail kebijakan 2327
Versi kebijakan 2327
Dokumen kebijakan JSON 2327
Pelajari selengkapnya 2328
AWSConfigServiceRolePolicy 2328
Menggunakan kebijakan ini 2328
Detail kebijakan 2328
Versi kebijakan 2328
Dokumen kebijakan JSON 2329
Pelajari selengkapnya 2388
AWSConfigThirdPartyServiceRolePolicy 2388
Menggunakan kebijakan ini 2388
Detail kebijakan 2388
Versi kebijakan 2389
Dokumen kebijakan JSON 2389
Pelajari selengkapnya 2390

AWSConfigUserAccess 2390
Menggunakan kebijakan ini 2390
Detail kebijakan 2390
Versi kebijakan 2391
Dokumen kebijakan JSON 2391
Pelajari selengkapnya 2391
AWSConnector 2392
Menggunakan kebijakan ini 2392
Detail kebijakan 2392
Versi kebijakan 2392
Dokumen kebijakan JSON 2392
Pelajari selengkapnya 2394
AWSControlTowerAccountServiceRolePolicy 2394
Menggunakan kebijakan ini 2395
Detail kebijakan 2395
Versi kebijakan 2395
Dokumen kebijakan JSON 2395
Pelajari selengkapnya 2400
AWSControlTowerCloudTrailRolePolicy 2401
Menggunakan kebijakan ini 2401
Detail kebijakan 2401
Versi kebijakan 2401
Dokumen kebijakan JSON 2401
Pelajari selengkapnya 2402
AWSControlTowerIdentityCenterManagementPolicy 2402
Menggunakan kebijakan ini 2402
Detail kebijakan 2402
Versi kebijakan 2403
Dokumen kebijakan JSON 2403
Pelajari selengkapnya 2404
AWSControlTowerServiceRolePolicy 2404
Menggunakan kebijakan ini 2404
Detail kebijakan 2404
Versi kebijakan 2405
Dokumen kebijakan JSON 2405
Pelajari selengkapnya 2410

AWSCostAndUsageReportAutomationPolicy 2411
Menggunakan kebijakan ini 2411
Detail kebijakan 2411
Versi kebijakan 2411
Dokumen kebijakan JSON 2411
Pelajari selengkapnya 2412
AWSDataExchangeDataGrantOwnerFullAccess 2413
Menggunakan kebijakan ini 2413
Detail kebijakan 2413
Versi kebijakan 2413
Dokumen kebijakan JSON 2413
Pelajari selengkapnya 2415
AWSDataExchangeDataGrantReceiverFullAccess 2415
Menggunakan kebijakan ini 2415
Detail kebijakan 2415
Versi kebijakan 2415
Dokumen kebijakan JSON 2416
Pelajari selengkapnya 2417
AWSDataExchangeFullAccess 2417
Menggunakan kebijakan ini 2418
Detail kebijakan 2418
Versi kebijakan 2418
Dokumen kebijakan JSON 2418
Pelajari selengkapnya 2421
AWSDataExchangeProviderFullAccess 2422
Menggunakan kebijakan ini 2422
Detail kebijakan 2422
Versi kebijakan 2422
Dokumen kebijakan JSON 2422
Pelajari selengkapnya 2426
AWSDataExchangeReadOnly 2426
Menggunakan kebijakan ini 2427
Detail kebijakan 2427
Versi kebijakan 2427
Dokumen kebijakan JSON 2427
Pelajari selengkapnya 2428

AWSDataExchangeServiceRolePolicyForLicenseManagement 2429
Menggunakan kebijakan ini 2429
Detail kebijakan 2429
Versi kebijakan 2429
Dokumen kebijakan JSON 2429
Pelajari selengkapnya 2430
AWSDataExchangeServiceRolePolicyForOrganizationDiscovery 2430
Menggunakan kebijakan ini 2430
Detail kebijakan 2430
Versi kebijakan 2431
Dokumen kebijakan JSON 2431
Pelajari selengkapnya 2431
AWSDataExchangeSubscriberFullAccess 2431
Menggunakan kebijakan ini 2432
Detail kebijakan 2432
Versi kebijakan 2432
Dokumen kebijakan JSON 2432
Pelajari selengkapnya 2434
AWSDataLifecycleManagerServiceRole 2435
Menggunakan kebijakan ini 2435
Detail kebijakan 2435
Versi kebijakan 2435
Dokumen kebijakan JSON 2435
Pelajari selengkapnya 2436
AWSDataLifecycleManagerServiceRoleForAMIManagement 2437
Menggunakan kebijakan ini 2437
Detail kebijakan 2437
Versi kebijakan 2437
Dokumen kebijakan JSON 2437
Pelajari selengkapnya 2439
AWSDataLifecycleManagerSSMFullAccess 2439
Menggunakan kebijakan ini 2439
Detail kebijakan 2439
Versi kebijakan 2439
Dokumen kebijakan JSON 2440
Pelajari selengkapnya 2441

AWSDataPipeline_FullAccess 2441
Menggunakan kebijakan ini 2441
Detail kebijakan 2441
Versi kebijakan 2442
Dokumen kebijakan JSON 2442
Pelajari selengkapnya 2443
AWSDataPipeline_PowerUser 2443
Menggunakan kebijakan ini 2443
Detail kebijakan 2443
Versi kebijakan 2443
Dokumen kebijakan JSON 2444
Pelajari selengkapnya 2444
AWSDataSyncDiscoveryServiceRolePolicy 2445
Menggunakan kebijakan ini 2445
Detail kebijakan 2445
Versi kebijakan 2445
Dokumen kebijakan JSON 2445
Pelajari selengkapnya 2446
AWSDataSyncFullAccess 2446
Menggunakan kebijakan ini 2447
Detail kebijakan 2447
Versi kebijakan 2447
Dokumen kebijakan JSON 2447
Pelajari selengkapnya 2450
AWSDataSyncReadOnlyAccess 2450
Menggunakan kebijakan ini 2450
Detail kebijakan 2450
Versi kebijakan 2450
Dokumen kebijakan JSON 2450
Pelajari selengkapnya 2451
AWSDataSyncServiceRolePolicy 2451
Menggunakan kebijakan ini 2451
Detail kebijakan 2452
Versi kebijakan 2452
Dokumen kebijakan JSON 2452
Pelajari selengkapnya 2453

AWSDeadlineCloud-FleetWorker 2453
Menggunakan kebijakan ini 2453
Detail kebijakan 2453
Versi kebijakan 2454
Dokumen kebijakan JSON 2454
Pelajari selengkapnya 2454
AWSDeadlineCloud-UserAccessFarms 2455
Menggunakan kebijakan ini 2455
Detail kebijakan 2455
Versi kebijakan 2455
Dokumen kebijakan JSON 2455
Pelajari selengkapnya 2462
AWSDeadlineCloud-UserAccessFleets 2462
Menggunakan kebijakan ini 2462
Detail kebijakan 2462
Versi kebijakan 2462
Dokumen kebijakan JSON 2463
Pelajari selengkapnya 2466
AWSDeadlineCloud-UserAccessJobs 2466
Menggunakan kebijakan ini 2467
Detail kebijakan 2467
Versi kebijakan 2467
Dokumen kebijakan JSON 2467
Pelajari selengkapnya 2471
AWSDeadlineCloud-UserAccessQueues 2471
Menggunakan kebijakan ini 2471
Detail kebijakan 2471
Versi kebijakan 2472
Dokumen kebijakan JSON 2472
Pelajari selengkapnya 2477
AWSDeadlineCloud-WorkerHost 2477
Menggunakan kebijakan ini 2477
Detail kebijakan 2477
Versi kebijakan 2477
Dokumen kebijakan JSON 2477
Pelajari selengkapnya 2479

AWSDeepLensLambdaFunctionAccessPolicy 2479
Menggunakan kebijakan ini 2479
Detail kebijakan 2479
Versi kebijakan 2479
Dokumen kebijakan JSON 2480
Pelajari selengkapnya 2481
AWSDeepLensServiceRolePolicy 2481
Menggunakan kebijakan ini 2481
Detail kebijakan 2481
Versi kebijakan 2482
Dokumen kebijakan JSON 2482
Pelajari selengkapnya 2489
AWSDeepRacerAccountAdminAccess 2489
Menggunakan kebijakan ini 2489
Detail kebijakan 2489
Versi kebijakan 2489
Dokumen kebijakan JSON 2490
Pelajari selengkapnya 2490
AWSDeepRacerCloudFormationAccessPolicy 2490
Menggunakan kebijakan ini 2491
Detail kebijakan 2491
Versi kebijakan 2491
Dokumen kebijakan JSON 2491
Pelajari selengkapnya 2494
AWSDeepRacerDefaultMultiUserAccess 2494
Menggunakan kebijakan ini 2494
Detail kebijakan 2494
Versi kebijakan 2495
Dokumen kebijakan JSON 2495
Pelajari selengkapnya 2496
AWSDeepRacerFullAccess 2497
Menggunakan kebijakan ini 2497
Detail kebijakan 2497
Versi kebijakan 2497
Dokumen kebijakan JSON 2497
Pelajari selengkapnya 2498

AWSDeepRacerRoboMakerAccessPolicy 2498
Menggunakan kebijakan ini 2499
Detail kebijakan 2499
Versi kebijakan 2499
Dokumen kebijakan JSON 2499
Pelajari selengkapnya 2501
AWSDeepRacerServiceRolePolicy 2501
Menggunakan kebijakan ini 2501
Detail kebijakan 2501
Versi kebijakan 2502
Dokumen kebijakan JSON 2502
Pelajari selengkapnya 2505
AWSDenyAll 2505
Menggunakan kebijakan ini 2505
Detail kebijakan 2505
Versi kebijakan 2506
Dokumen kebijakan JSON 2506
Pelajari selengkapnya 2506
AWSDeviceFarmFullAccess 2506
Menggunakan kebijakan ini 2507
Detail kebijakan 2507
Versi kebijakan 2507
Dokumen kebijakan JSON 2507
Pelajari selengkapnya 2507
AWSDeviceFarmServiceRolePolicy 2508
Menggunakan kebijakan ini 2508
Detail kebijakan 2508
Versi kebijakan 2508
Dokumen kebijakan JSON 2508
Pelajari selengkapnya 2510
AWSDeviceFarmTestGridServiceRolePolicy 2511
Menggunakan kebijakan ini 2511
Detail kebijakan 2511
Versi kebijakan 2511
Dokumen kebijakan JSON 2511
Pelajari selengkapnya 2513

AWSDirectConnectFullAccess 2513
Menggunakan kebijakan ini 2514
Detail kebijakan 2514
Versi kebijakan 2514
Dokumen kebijakan JSON 2514
Pelajari selengkapnya 2514
AWSDirectConnectReadOnlyAccess 2515
Menggunakan kebijakan ini 2515
Detail kebijakan 2515
Versi kebijakan 2515
Dokumen kebijakan JSON 2515
Pelajari selengkapnya 2516
AWSDirectConnectServiceRolePolicy 2516
Menggunakan kebijakan ini 2516
Detail kebijakan 2516
Versi kebijakan 2517
Dokumen kebijakan JSON 2517
Pelajari selengkapnya 2517
AWSDirectoryServiceDataFullAccess 2517
Menggunakan kebijakan ini 2518
Detail kebijakan 2518
Versi kebijakan 2518
Dokumen kebijakan JSON 2518
Pelajari selengkapnya 2519
AWSDirectoryServiceDataReadOnlyAccess 2519
Menggunakan kebijakan ini 2519
Detail kebijakan 2519
Versi kebijakan 2520
Dokumen kebijakan JSON 2520
Pelajari selengkapnya 2520
AWSDirectoryServiceFullAccess 2521
Menggunakan kebijakan ini 2521
Detail kebijakan 2521
Versi kebijakan 2521
Dokumen kebijakan JSON 2521
Pelajari selengkapnya 2523

AWSDirectoryServiceReadOnlyAccess 2523
Menggunakan kebijakan ini 2523
Detail kebijakan 2524
Versi kebijakan 2524
Dokumen kebijakan JSON 2524
Pelajari selengkapnya 2525
AWSDirectoryServiceServiceRolePolicy 2525
Menggunakan kebijakan ini 2525
Detail kebijakan 2525
Versi kebijakan 2525
Dokumen kebijakan JSON 2526
Pelajari selengkapnya 2527
AWSDiscoveryContinuousExportFirehosePolicy 2527
Menggunakan kebijakan ini 2527
Detail kebijakan 2527
Versi kebijakan 2527
Dokumen kebijakan JSON 2527
Pelajari selengkapnya 2528
AWSDMSFleetAdvisorServiceRolePolicy 2529
Menggunakan kebijakan ini 2529
Detail kebijakan 2529
Versi kebijakan 2529
Dokumen kebijakan JSON 2529
Pelajari selengkapnya 2530
AWSDMSServerlessServiceRolePolicy 2530
Menggunakan kebijakan ini 2530
Detail kebijakan 2530
Versi kebijakan 2530
Dokumen kebijakan JSON 2531
Pelajari selengkapnya 2533
AWSEC2CapacityManagerServiceRolePolicy 2533
Menggunakan kebijakan ini 2534
Detail kebijakan 2534
Versi kebijakan 2534
Dokumen kebijakan JSON 2534
Pelajari selengkapnya 2535

AWSEC2CapacityReservationFleetRolePolicy 2535
Menggunakan kebijakan ini 2535
Detail kebijakan 2535
Versi kebijakan 2536
Dokumen kebijakan JSON 2536
Pelajari selengkapnya 2537
AWSEC2FleetServiceRolePolicy 2537
Menggunakan kebijakan ini 2537
Detail kebijakan 2537
Versi kebijakan 2538
Dokumen kebijakan JSON 2538
Pelajari selengkapnya 2540
AWSEC2SpotFleetServiceRolePolicy 2540
Menggunakan kebijakan ini 2540
Detail kebijakan 2540
Versi kebijakan 2540
Dokumen kebijakan JSON 2541
Pelajari selengkapnya 2543
AWSEC2SpotServiceRolePolicy 2543
Menggunakan kebijakan ini 2543
Detail kebijakan 2543
Versi kebijakan 2543
Dokumen kebijakan JSON 2543
Pelajari selengkapnya 2545
AWSEC2SqlHaInstancePolicy 2545
Menggunakan kebijakan ini 2545
Detail kebijakan 2545
Versi kebijakan 2545
Dokumen kebijakan JSON 2546
Pelajari selengkapnya 2547
AWSEC2SqlHaServiceRolePolicy 2547
Menggunakan kebijakan ini 2547
Detail kebijakan 2547
Versi kebijakan 2548
Dokumen kebijakan JSON 2548
Pelajari selengkapnya 2550

AWSEC2VssRestorePolicy 2550
Menggunakan kebijakan ini 2550
Detail kebijakan 2550
Versi kebijakan 2550
Dokumen kebijakan JSON 2550
Pelajari selengkapnya 2553
AWSEC2VssSnapshotPolicy 2553
Menggunakan kebijakan ini 2553
Detail kebijakan 2553
Versi kebijakan 2554
Dokumen kebijakan JSON 2554
Pelajari selengkapnya 2557
AWSECRPullThroughCache_ServiceRolePolicy 2557
Menggunakan kebijakan ini 2557
Detail kebijakan 2557
Versi kebijakan 2558
Dokumen kebijakan JSON 2558
Pelajari selengkapnya 2559
AWSElasticBeanstalkCustomPlatformforEC2Role 2559
Menggunakan kebijakan ini 2559
Detail kebijakan 2559
Versi kebijakan 2560
Dokumen kebijakan JSON 2560
Pelajari selengkapnya 2561
AWSElasticBeanstalkEKSImageBuild 2562
Menggunakan kebijakan ini 2562
Detail kebijakan 2562
Versi kebijakan 2562
Dokumen kebijakan JSON 2562
Pelajari selengkapnya 2564
AWSElasticBeanstalkEKSObservability 2564
Menggunakan kebijakan ini 2565
Detail kebijakan 2565
Versi kebijakan 2565
Dokumen kebijakan JSON 2565
Pelajari selengkapnya 2567

AWSElasticBeanstalkEKSTagging 2567
Menggunakan kebijakan ini 2567
Detail kebijakan 2567
Versi kebijakan 2567
Dokumen kebijakan JSON 2568
Pelajari selengkapnya 2570
AWSElasticBeanstalkEnhancedHealth 2570
Menggunakan kebijakan ini 2571
Detail kebijakan 2571
Versi kebijakan 2571
Dokumen kebijakan JSON 2571
Pelajari selengkapnya 2572
AWSElasticBeanstalkMaintenance 2572
Menggunakan kebijakan ini 2572
Detail kebijakan 2573
Versi kebijakan 2573
Dokumen kebijakan JSON 2573
Pelajari selengkapnya 2574
AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy 2574
Menggunakan kebijakan ini 2574
Detail kebijakan 2574
Versi kebijakan 2575
Dokumen kebijakan JSON 2575
Pelajari selengkapnya 2582
AWSElasticBeanstalkManagedUpdatesServiceRolePolicy 2582
Menggunakan kebijakan ini 2582
Detail kebijakan 2582
Versi kebijakan 2582
Dokumen kebijakan JSON 2583
Pelajari selengkapnya 2588
AWSElasticBeanstalkMulticontainerDocker 2588
Menggunakan kebijakan ini 2589
Detail kebijakan 2589
Versi kebijakan 2589
Dokumen kebijakan JSON 2589
Pelajari selengkapnya 2591

AWSElasticBeanstalkReadOnly 2591
Menggunakan kebijakan ini 2591
Detail kebijakan 2592
Versi kebijakan 2592
Dokumen kebijakan JSON 2592
Pelajari selengkapnya 2594
AWSElasticBeanstalkRoleCore 2595
Menggunakan kebijakan ini 2595
Detail kebijakan 2595
Versi kebijakan 2595
Dokumen kebijakan JSON 2595
Pelajari selengkapnya 2600
AWSElasticBeanstalkRoleCWL 2600
Menggunakan kebijakan ini 2601
Detail kebijakan 2601
Versi kebijakan 2601
Dokumen kebijakan JSON 2601
Pelajari selengkapnya 2602
AWSElasticBeanstalkRoleECS 2602
Menggunakan kebijakan ini 2602
Detail kebijakan 2602
Versi kebijakan 2602
Dokumen kebijakan JSON 2602
Pelajari selengkapnya 2603
AWSElasticBeanstalkRoleRDS 2604
Menggunakan kebijakan ini 2604
Detail kebijakan 2604
Versi kebijakan 2604
Dokumen kebijakan JSON 2604
Pelajari selengkapnya 2605
AWSElasticBeanstalkRoleSNS 2605
Menggunakan kebijakan ini 2605
Detail kebijakan 2605
Versi kebijakan 2605
Dokumen kebijakan JSON 2606
Pelajari selengkapnya 2606

AWSElasticBeanstalkRoleWorkerTier 2607
Menggunakan kebijakan ini 2607
Detail kebijakan 2607
Versi kebijakan 2607
Dokumen kebijakan JSON 2607
Pelajari selengkapnya 2608
AWSElasticBeanstalkService 2608
Menggunakan kebijakan ini 2608
Detail kebijakan 2609
Versi kebijakan 2609
Dokumen kebijakan JSON 2609
Pelajari selengkapnya 2613
AWSElasticBeanstalkServiceRolePolicy 2613
Menggunakan kebijakan ini 2614
Detail kebijakan 2614
Versi kebijakan 2614
Dokumen kebijakan JSON 2614
Pelajari selengkapnya 2628
AWSElasticBeanstalkWebTier 2628
Menggunakan kebijakan ini 2628
Detail kebijakan 2628
Versi kebijakan 2628
Dokumen kebijakan JSON 2629
Pelajari selengkapnya 2631
AWSElasticBeanstalkWorkerTier 2631
Menggunakan kebijakan ini 2631
Detail kebijakan 2632
Versi kebijakan 2632
Dokumen kebijakan JSON 2632
Pelajari selengkapnya 2635
AWSElasticDisasterRecoveryAgentInstallationPolicy 2635
Menggunakan kebijakan ini 2636
Detail kebijakan 2636
Versi kebijakan 2636
Dokumen kebijakan JSON 2636
Pelajari selengkapnya 2638

AWSElasticDisasterRecoveryAgentPolicy 2638
Menggunakan kebijakan ini 2638
Detail kebijakan 2638
Versi kebijakan 2638
Dokumen kebijakan JSON 2639
Pelajari selengkapnya 2639
AWSElasticDisasterRecoveryConsoleFullAccess 2640
Menggunakan kebijakan ini 2640
Detail kebijakan 2640
Versi kebijakan 2640
Dokumen kebijakan JSON 2640
Pelajari selengkapnya 2650
AWSElasticDisasterRecoveryConsoleFullAccess_v2 2651
Menggunakan kebijakan ini 2651
Detail kebijakan 2651
Versi kebijakan 2651
Dokumen kebijakan JSON 2651
Pelajari selengkapnya 2667
AWSElasticDisasterRecoveryConversionServerPolicy 2667
Menggunakan kebijakan ini 2667
Detail kebijakan 2668
Versi kebijakan 2668
Dokumen kebijakan JSON 2668
Pelajari selengkapnya 2669
AWSElasticDisasterRecoveryCrossAccountReplicationPolicy 2669
Menggunakan kebijakan ini 2669
Detail kebijakan 2669
Versi kebijakan 2669
Dokumen kebijakan JSON 2670
Pelajari selengkapnya 2670
AWSElasticDisasterRecoveryEc2InstancePolicy 2671
Menggunakan kebijakan ini 2671
Detail kebijakan 2671
Versi kebijakan 2671
Dokumen kebijakan JSON 2671
Pelajari selengkapnya 2673

AWSElasticDisasterRecoveryFailbackInstallationPolicy 2673
Menggunakan kebijakan ini 2674
Detail kebijakan 2674
Versi kebijakan 2674
Dokumen kebijakan JSON 2674
Pelajari selengkapnya 2675
AWSElasticDisasterRecoveryFailbackPolicy 2675
Menggunakan kebijakan ini 2675
Detail kebijakan 2676
Versi kebijakan 2676
Dokumen kebijakan JSON 2676
Pelajari selengkapnya 2677
AWSElasticDisasterRecoveryLaunchActionsPolicy 2678
Menggunakan kebijakan ini 2678
Detail kebijakan 2678
Versi kebijakan 2678
Dokumen kebijakan JSON 2678
Pelajari selengkapnya 2684
AWSElasticDisasterRecoveryNetworkReplicationPolicy 2685
Menggunakan kebijakan ini 2685
Detail kebijakan 2685
Versi kebijakan 2685
Dokumen kebijakan JSON 2685
Pelajari selengkapnya 2686
AWSElasticDisasterRecoveryReadOnlyAccess 2686
Menggunakan kebijakan ini 2686
Detail kebijakan 2687
Versi kebijakan 2687
Dokumen kebijakan JSON 2687
Pelajari selengkapnya 2689
AWSElasticDisasterRecoveryRecoveryInstancePolicy 2690
Menggunakan kebijakan ini 2690
Detail kebijakan 2690
Versi kebijakan 2690
Dokumen kebijakan JSON 2690
Pelajari selengkapnya 2693

AWSElasticDisasterRecoveryReplicationServerPolicy 2693
Menggunakan kebijakan ini 2694
Detail kebijakan 2694
Versi kebijakan 2694
Dokumen kebijakan JSON 2694
Pelajari selengkapnya 2696
AWSElasticDisasterRecoveryServiceRolePolicy 2696
Menggunakan kebijakan ini 2697
Detail kebijakan 2697
Versi kebijakan 2697
Dokumen kebijakan JSON 2697
Pelajari selengkapnya 2707
AWSElasticDisasterRecoveryStagingAccountPolicy 2707
Menggunakan kebijakan ini 2707
Detail kebijakan 2708
Versi kebijakan 2708
Dokumen kebijakan JSON 2708
Pelajari selengkapnya 2709
AWSElasticDisasterRecoveryStagingAccountPolicy_v2 2709
Menggunakan kebijakan ini 2709
Detail kebijakan 2709
Versi kebijakan 2710
Dokumen kebijakan JSON 2710
Pelajari selengkapnya 2711
AWSElasticLoadBalancingClassicServiceRolePolicy 2711
Menggunakan kebijakan ini 2712
Detail kebijakan 2712
Versi kebijakan 2712
Dokumen kebijakan JSON 2712
Pelajari selengkapnya 2713
AWSElasticLoadBalancingServiceRolePolicy 2713
Menggunakan kebijakan ini 2713
Detail kebijakan 2713
Versi kebijakan 2714
Dokumen kebijakan JSON 2714
Pelajari selengkapnya 2715

AWSElementalMediaConnectCreateBridge 2715
Menggunakan kebijakan ini 2715
Detail kebijakan 2715
Versi kebijakan 2716
Dokumen kebijakan JSON 2716
Pelajari selengkapnya 2716
AWSElementalMediaConnectCreateFlow 2717
Menggunakan kebijakan ini 2717
Detail kebijakan 2717
Versi kebijakan 2717
Dokumen kebijakan JSON 2717
Pelajari selengkapnya 2718
AWSElementalMediaConnectDeleteBridge 2718
Menggunakan kebijakan ini 2719
Detail kebijakan 2719
Versi kebijakan 2719
Dokumen kebijakan JSON 2719
Pelajari selengkapnya 2720
AWSElementalMediaConnectDeleteFlow 2720
Menggunakan kebijakan ini 2720
Detail kebijakan 2720
Versi kebijakan 2720
Dokumen kebijakan JSON 2721
Pelajari selengkapnya 2721
AWSElementalMediaConnectFullAccess 2721
Menggunakan kebijakan ini 2722
Detail kebijakan 2722
Versi kebijakan 2722
Dokumen kebijakan JSON 2722
Pelajari selengkapnya 2722
AWSElementalMediaConnectReadOnlyAccess 2723
Menggunakan kebijakan ini 2723
Detail kebijakan 2723
Versi kebijakan 2723
Dokumen kebijakan JSON 2723
Pelajari selengkapnya 2724

AWSElementalMediaConvertFullAccess 2724
Menggunakan kebijakan ini 2724
Detail kebijakan 2725
Versi kebijakan 2725
Dokumen kebijakan JSON 2725
Pelajari selengkapnya 2726
AWSElementalMediaConvertReadOnly 2726
Menggunakan kebijakan ini 2726
Detail kebijakan 2726
Versi kebijakan 2726
Dokumen kebijakan JSON 2727
Pelajari selengkapnya 2727
AWSElementalMediaLiveFullAccess 2727
Menggunakan kebijakan ini 2728
Detail kebijakan 2728
Versi kebijakan 2728
Dokumen kebijakan JSON 2728
Pelajari selengkapnya 2728
AWSElementalMediaLiveReadOnly 2729
Menggunakan kebijakan ini 2729
Detail kebijakan 2729
Versi kebijakan 2729
Dokumen kebijakan JSON 2729
Pelajari selengkapnya 2730
AWSElementalMediaPackageFullAccess 2730
Menggunakan kebijakan ini 2730
Detail kebijakan 2730
Versi kebijakan 2730
Dokumen kebijakan JSON 2731
Pelajari selengkapnya 2731
AWSElementalMediaPackageReadOnly 2731
Menggunakan kebijakan ini 2731
Detail kebijakan 2731
Versi kebijakan 2732
Dokumen kebijakan JSON 2732
Pelajari selengkapnya 2732

AWSElementalMediaPackageV2FullAccess 2732
Menggunakan kebijakan ini 2733
Detail kebijakan 2733
Versi kebijakan 2733
Dokumen kebijakan JSON 2733
Pelajari selengkapnya 2733
AWSElementalMediaPackageV2ReadOnly 2734
Menggunakan kebijakan ini 2734
Detail kebijakan 2734
Versi kebijakan 2734
Dokumen kebijakan JSON 2734
Pelajari selengkapnya 2735
AWSElementalMediaStoreFullAccess 2735
Menggunakan kebijakan ini 2735
Detail kebijakan 2735
Versi kebijakan 2735
Dokumen kebijakan JSON 2735
Pelajari selengkapnya 2736
AWSElementalMediaStoreReadOnly 2736
Menggunakan kebijakan ini 2736
Detail kebijakan 2736
Versi kebijakan 2737
Dokumen kebijakan JSON 2737
Pelajari selengkapnya 2737
AWSElementalMediaTailorFullAccess 2738
Menggunakan kebijakan ini 2738
Detail kebijakan 2738
Versi kebijakan 2738
Dokumen kebijakan JSON 2738
Pelajari selengkapnya 2739
AWSElementalMediaTailorReadOnly 2739
Menggunakan kebijakan ini 2739
Detail kebijakan 2739
Versi kebijakan 2739
Dokumen kebijakan JSON 2739
Pelajari selengkapnya 2740

AWSEnhancedClassicNetworkingMangementPolicy 2740
Menggunakan kebijakan ini 2740
Detail kebijakan 2740
Versi kebijakan 2741
Dokumen kebijakan JSON 2741
Pelajari selengkapnya 2741
AWSEntityResolutionConsoleFullAccess 2741
Menggunakan kebijakan ini 2741
Detail kebijakan 2742
Versi kebijakan 2742
Dokumen kebijakan JSON 2742
Pelajari selengkapnya 2745
AWSEntityResolutionConsoleReadOnlyAccess 2745
Menggunakan kebijakan ini 2746
Detail kebijakan 2746
Versi kebijakan 2746
Dokumen kebijakan JSON 2746
Pelajari selengkapnya 2747
AWSFaultInjectionSimulatorEC2Access 2747
Menggunakan kebijakan ini 2747
Detail kebijakan 2747
Versi kebijakan 2747
Dokumen kebijakan JSON 2748
Pelajari selengkapnya 2749
AWSFaultInjectionSimulatorECSAccess 2749
Menggunakan kebijakan ini 2750
Detail kebijakan 2750
Versi kebijakan 2750
Dokumen kebijakan JSON 2750
Pelajari selengkapnya 2752
AWSFaultInjectionSimulatorEKSAccess 2752
Menggunakan kebijakan ini 2753
Detail kebijakan 2753
Versi kebijakan 2753
Dokumen kebijakan JSON 2753
Pelajari selengkapnya 2754

AWSFaultInjectionSimulatorNetworkAccess 2754
Menggunakan kebijakan ini 2755
Detail kebijakan 2755
Versi kebijakan 2755
Dokumen kebijakan JSON 2755
Pelajari selengkapnya 2762
AWSFaultInjectionSimulatorRDSAccess 2762
Menggunakan kebijakan ini 2762
Detail kebijakan 2763
Versi kebijakan 2763
Dokumen kebijakan JSON 2763
Pelajari selengkapnya 2764
AWSFaultInjectionSimulatorSSMAccess 2764
Menggunakan kebijakan ini 2764
Detail kebijakan 2765
Versi kebijakan 2765
Dokumen kebijakan JSON 2765
Pelajari selengkapnya 2766
AWSFinSpaceServiceRolePolicy 2767
Menggunakan kebijakan ini 2767
Detail kebijakan 2767
Versi kebijakan 2767
Dokumen kebijakan JSON 2767
Pelajari selengkapnya 2768
AWSFMAdminFullAccess 2768
Menggunakan kebijakan ini 2768
Detail kebijakan 2768
Versi kebijakan 2768
Dokumen kebijakan JSON 2769
Pelajari selengkapnya 2770
AWSFMAdminReadOnlyAccess 2771
Menggunakan kebijakan ini 2771
Detail kebijakan 2771
Versi kebijakan 2771
Dokumen kebijakan JSON 2771
Pelajari selengkapnya 2773

AWSFMMemberReadOnlyAccess 2773
Menggunakan kebijakan ini 2773
Detail kebijakan 2773
Versi kebijakan 2773
Dokumen kebijakan JSON 2774
Pelajari selengkapnya 2774
AWSForWordPressPluginPolicy 2774
Menggunakan kebijakan ini 2774
Detail kebijakan 2775
Versi kebijakan 2775
Dokumen kebijakan JSON 2775
Pelajari selengkapnya 2777
AWSGitSyncServiceRolePolicy 2778
Menggunakan kebijakan ini 2778
Detail kebijakan 2778
Versi kebijakan 2778
Dokumen kebijakan JSON 2778
Pelajari selengkapnya 2779
AWSGlobalAcceleratorSLRPolicy 2779
Menggunakan kebijakan ini 2779
Detail kebijakan 2779
Versi kebijakan 2780
Dokumen kebijakan JSON 2780
Pelajari selengkapnya 2781
AWSGlueConsoleFullAccess 2781
Menggunakan kebijakan ini 2782
Detail kebijakan 2782
Versi kebijakan 2782
Dokumen kebijakan JSON 2782
Pelajari selengkapnya 2787
AWSGlueConsoleSageMakerNotebookFullAccess 2787
Menggunakan kebijakan ini 2787
Detail kebijakan 2787
Versi kebijakan 2787
Dokumen kebijakan JSON 2788
Pelajari selengkapnya 2793

AwsGlueDataBrewFullAccessPolicy 2793
Menggunakan kebijakan ini 2793
Detail kebijakan 2794
Versi kebijakan 2794
Dokumen kebijakan JSON 2794
Pelajari selengkapnya 2799
AWSGlueDataBrewServiceRole 2799
Menggunakan kebijakan ini 2799
Detail kebijakan 2800
Versi kebijakan 2800
Dokumen kebijakan JSON 2800
Pelajari selengkapnya 2803
AWSGlueSchemaRegistryFullAccess 2803
Menggunakan kebijakan ini 2803
Detail kebijakan 2803
Versi kebijakan 2803
Dokumen kebijakan JSON 2804
Pelajari selengkapnya 2805
AWSGlueSchemaRegistryReadonlyAccess 2805
Menggunakan kebijakan ini 2805
Detail kebijakan 2805
Versi kebijakan 2806
Dokumen kebijakan JSON 2806
Pelajari selengkapnya 2806
AWSGlueServiceNotebookRole 2807
Menggunakan kebijakan ini 2807
Detail kebijakan 2807
Versi kebijakan 2807
Dokumen kebijakan JSON 2807
Pelajari selengkapnya 2810
AWSGlueServiceRole 2810
Menggunakan kebijakan ini 2810
Detail kebijakan 2810
Versi kebijakan 2810
Dokumen kebijakan JSON 2810
Pelajari selengkapnya 2813

AwsGlueSessionUserRestrictedNotebookPolicy 2813
Menggunakan kebijakan ini 2813
Detail kebijakan 2813
Versi kebijakan 2813
Dokumen kebijakan JSON 2814
Pelajari selengkapnya 2816
AwsGlueSessionUserRestrictedNotebookServiceRole 2817
Menggunakan kebijakan ini 2817
Detail kebijakan 2817
Versi kebijakan 2817
Dokumen kebijakan JSON 2817
Pelajari selengkapnya 2821
AwsGlueSessionUserRestrictedPolicy 2821
Menggunakan kebijakan ini 2822
Detail kebijakan 2822
Versi kebijakan 2822
Dokumen kebijakan JSON 2822
Pelajari selengkapnya 2825
AwsGlueSessionUserRestrictedServiceRole 2825
Menggunakan kebijakan ini 2825
Detail kebijakan 2825
Versi kebijakan 2826
Dokumen kebijakan JSON 2826
Pelajari selengkapnya 2830
AWSGrafanaAccountAdministrator 2830
Menggunakan kebijakan ini 2831
Detail kebijakan 2831
Versi kebijakan 2831
Dokumen kebijakan JSON 2831
Pelajari selengkapnya 2832
AWSGrafanaConsoleReadOnlyAccess 2832
Menggunakan kebijakan ini 2832
Detail kebijakan 2833
Versi kebijakan 2833
Dokumen kebijakan JSON 2833
Pelajari selengkapnya 2833

AWSGrafanaWorkspacePermissionManagement 2834
Menggunakan kebijakan ini 2834
Detail kebijakan 2834
Versi kebijakan 2834
Dokumen kebijakan JSON 2834
Pelajari selengkapnya 2835
AWSGrafanaWorkspacePermissionManagementV2 2835
Menggunakan kebijakan ini 2836
Detail kebijakan 2836
Versi kebijakan 2836
Dokumen kebijakan JSON 2836
Pelajari selengkapnya 2837
AWSGreengrassFullAccess 2837
Menggunakan kebijakan ini 2837
Detail kebijakan 2837
Versi kebijakan 2838
Dokumen kebijakan JSON 2838
Pelajari selengkapnya 2838
AWSGreengrassReadOnlyAccess 2838
Menggunakan kebijakan ini 2839
Detail kebijakan 2839
Versi kebijakan 2839
Dokumen kebijakan JSON 2839
Pelajari selengkapnya 2839
AWSGreengrassResourceAccessRolePolicy 2840
Menggunakan kebijakan ini 2840
Detail kebijakan 2840
Versi kebijakan 2840
Dokumen kebijakan JSON 2840
Pelajari selengkapnya 2843
AWSGroundStationAgentInstancePolicy 2843
Menggunakan kebijakan ini 2843
Detail kebijakan 2843
Versi kebijakan 2843
Dokumen kebijakan JSON 2844
Pelajari selengkapnya 2844

AWSHealth_EventProcessorServiceRolePolicy 2844
Menggunakan kebijakan ini 2844
Detail kebijakan 2844
Versi kebijakan 2845
Dokumen kebijakan JSON 2845
Pelajari selengkapnya 2846
AWSHealthFullAccess 2846
Menggunakan kebijakan ini 2846
Detail kebijakan 2846
Versi kebijakan 2846
Dokumen kebijakan JSON 2846
Pelajari selengkapnya 2847
AWSHealthImagingFullAccess 2848
Menggunakan kebijakan ini 2848
Detail kebijakan 2848
Versi kebijakan 2848
Dokumen kebijakan JSON 2848
Pelajari selengkapnya 2849
AWSHealthImagingReadOnlyAccess 2849
Menggunakan kebijakan ini 2849
Detail kebijakan 2849
Versi kebijakan 2850
Dokumen kebijakan JSON 2850
Pelajari selengkapnya 2850
AWSHealthImagingServiceRolePolicy 2851
Menggunakan kebijakan ini 2851
Detail kebijakan 2851
Versi kebijakan 2851
Dokumen kebijakan JSON 2851
Pelajari selengkapnya 2852
AWSHealthOmicsServiceLinkedRolePolicy 2852
Menggunakan kebijakan ini 2852
Detail kebijakan 2852
Versi kebijakan 2852
Dokumen kebijakan JSON 2853
Pelajari selengkapnya 2855

AWSIAMIdentityCenterAllowListForIdentityContext 2855
Menggunakan kebijakan ini 2855
Detail kebijakan 2855
Versi kebijakan 2855
Dokumen kebijakan JSON 2856
Pelajari selengkapnya 2859
AWSIAMRoleManagerServiceRolePolicy 2859
Menggunakan kebijakan ini 2859
Detail kebijakan 2859
Versi kebijakan 2859
Dokumen kebijakan JSON 2860
Pelajari selengkapnya 2860
AWSIdentityCenterExternalManagementPolicy 2860
Menggunakan kebijakan ini 2861
Detail kebijakan 2861
Versi kebijakan 2861
Dokumen kebijakan JSON 2861
Pelajari selengkapnya 2863
AWSIdentitySyncFullAccess 2863
Menggunakan kebijakan ini 2863
Detail kebijakan 2863
Versi kebijakan 2863
Dokumen kebijakan JSON 2864
Pelajari selengkapnya 2864
AWSIdentitySyncReadOnlyAccess 2865
Menggunakan kebijakan ini 2865
Detail kebijakan 2865
Versi kebijakan 2865
Dokumen kebijakan JSON 2865
Pelajari selengkapnya 2866
AWSImageBuilderFullAccess 2866
Menggunakan kebijakan ini 2866
Detail kebijakan 2866
Versi kebijakan 2866
Dokumen kebijakan JSON 2867
Pelajari selengkapnya 2869

AWSImageBuilderReadOnlyAccess 2870
Menggunakan kebijakan ini 2870
Detail kebijakan 2870
Versi kebijakan 2870
Dokumen kebijakan JSON 2870
Pelajari selengkapnya 2871
AWSImportExportFullAccess 2871
Menggunakan kebijakan ini 2871
Detail kebijakan 2871
Versi kebijakan 2871
Dokumen kebijakan JSON 2872
Pelajari selengkapnya 2872
AWSImportExportReadOnlyAccess 2872
Menggunakan kebijakan ini 2872
Detail kebijakan 2873
Versi kebijakan 2873
Dokumen kebijakan JSON 2873
Pelajari selengkapnya 2873
AWSIncidentManagerIncidentAccessServiceRolePolicy 2874
Menggunakan kebijakan ini 2874
Detail kebijakan 2874
Versi kebijakan 2874
Dokumen kebijakan JSON 2874
Pelajari selengkapnya 2875
AWSIncidentManagerResolverAccess 2875
Menggunakan kebijakan ini 2875
Detail kebijakan 2875
Versi kebijakan 2876
Dokumen kebijakan JSON 2876
Pelajari selengkapnya 2877
AWSIncidentManagerServiceRolePolicy 2877
Menggunakan kebijakan ini 2877
Detail kebijakan 2877
Versi kebijakan 2878
Dokumen kebijakan JSON 2878
Pelajari selengkapnya 2879

AWSIoT1ClickFullAccess 2879
Menggunakan kebijakan ini 2879
Detail kebijakan 2879
Versi kebijakan 2879
Dokumen kebijakan JSON 2880
Pelajari selengkapnya 2880
AWSIoT1ClickReadOnlyAccess 2880
Menggunakan kebijakan ini 2880
Detail kebijakan 2880
Versi kebijakan 2881
Dokumen kebijakan JSON 2881
Pelajari selengkapnya 2881
AWSIoTAnalyticsFullAccess 2882
Menggunakan kebijakan ini 2882
Detail kebijakan 2882
Versi kebijakan 2882
Dokumen kebijakan JSON 2882
Pelajari selengkapnya 2883
AWSIoTAnalyticsReadOnlyAccess 2883
Menggunakan kebijakan ini 2883
Detail kebijakan 2883
Versi kebijakan 2883
Dokumen kebijakan JSON 2883
Pelajari selengkapnya 2884
AWSIoTConfigAccess 2884
Menggunakan kebijakan ini 2884
Detail kebijakan 2884
Versi kebijakan 2885
Dokumen kebijakan JSON 2885
Pelajari selengkapnya 2889
AWSIoTConfigReadOnlyAccess 2889
Menggunakan kebijakan ini 2889
Detail kebijakan 2889
Versi kebijakan 2889
Dokumen kebijakan JSON 2889
Pelajari selengkapnya 2891

AWSIoTDataAccess 2892
Menggunakan kebijakan ini 2892
Detail kebijakan 2892
Versi kebijakan 2892
Dokumen kebijakan JSON 2892
Pelajari selengkapnya 2893
AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction 2893
Menggunakan kebijakan ini 2893
Detail kebijakan 2893
Versi kebijakan 2894
Dokumen kebijakan JSON 2894
Pelajari selengkapnya 2894
AWSIoTDeviceDefenderAudit 2894
Menggunakan kebijakan ini 2895
Detail kebijakan 2895
Versi kebijakan 2895
Dokumen kebijakan JSON 2895
Pelajari selengkapnya 2896
AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction 2896
Menggunakan kebijakan ini 2896
Detail kebijakan 2896
Versi kebijakan 2897
Dokumen kebijakan JSON 2897
Pelajari selengkapnya 2898
AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction 2898
Menggunakan kebijakan ini 2898
Detail kebijakan 2898
Versi kebijakan 2898
Dokumen kebijakan JSON 2899
Pelajari selengkapnya 2899
AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction 2899
Menggunakan kebijakan ini 2900
Detail kebijakan 2900
Versi kebijakan 2900
Dokumen kebijakan JSON 2900
Pelajari selengkapnya 2901

AWSIoTDeviceDefenderUpdateCACertMitigationAction 2901
Menggunakan kebijakan ini 2901
Detail kebijakan 2901
Versi kebijakan 2901
Dokumen kebijakan JSON 2902
Pelajari selengkapnya 2902
AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction 2902
Menggunakan kebijakan ini 2902
Detail kebijakan 2903
Versi kebijakan 2903
Dokumen kebijakan JSON 2903
Pelajari selengkapnya 2903
AWSIoTDeviceTesterForFreeRTOSFullAccess 2904
Menggunakan kebijakan ini 2904
Detail kebijakan 2904
Versi kebijakan 2904
Dokumen kebijakan JSON 2904
Pelajari selengkapnya 2910
AWSIoTDeviceTesterForGreengrassFullAccess 2911
Menggunakan kebijakan ini 2911
Detail kebijakan 2911
Versi kebijakan 2911
Dokumen kebijakan JSON 2911
Pelajari selengkapnya 2914
AWSIoTEventsFullAccess 2914
Menggunakan kebijakan ini 2915
Detail kebijakan 2915
Versi kebijakan 2915
Dokumen kebijakan JSON 2915
Pelajari selengkapnya 2915
AWSIoTEventsReadOnlyAccess 2916
Menggunakan kebijakan ini 2916
Detail kebijakan 2916
Versi kebijakan 2916
Dokumen kebijakan JSON 2916
Pelajari selengkapnya 2917

AWSIoTFleetHubFederationAccess 2917
Menggunakan kebijakan ini 2917
Detail kebijakan 2917
Versi kebijakan 2917
Dokumen kebijakan JSON 2918
Pelajari selengkapnya 2919
AWSIoTFleetwiseServiceRolePolicy 2920
Menggunakan kebijakan ini 2920
Detail kebijakan 2920
Versi kebijakan 2920
Dokumen kebijakan JSON 2920
Pelajari selengkapnya 2921
AWSIoTFullAccess 2921
Menggunakan kebijakan ini 2921
Detail kebijakan 2921
Versi kebijakan 2921
Dokumen kebijakan JSON 2922
Pelajari selengkapnya 2922
AWSIoTLogging 2922
Menggunakan kebijakan ini 2922
Detail kebijakan 2923
Versi kebijakan 2923
Dokumen kebijakan JSON 2923
Pelajari selengkapnya 2924
AWSIoTManagedIntegrationsFullAccess 2924
Menggunakan kebijakan ini 2924
Detail kebijakan 2924
Versi kebijakan 2924
Dokumen kebijakan JSON 2924
Pelajari selengkapnya 2925
AWSIoTManagedIntegrationsRolePolicy 2925
Menggunakan kebijakan ini 2925
Detail kebijakan 2926
Versi kebijakan 2926
Dokumen kebijakan JSON 2926
Pelajari selengkapnya 2927

AWSIoTOTAUpdate 2927
Menggunakan kebijakan ini 2928
Detail kebijakan 2928
Versi kebijakan 2928
Dokumen kebijakan JSON 2928
Pelajari selengkapnya 2928
AWSIotRoboRunnerFullAccess 2929
Menggunakan kebijakan ini 2929
Detail kebijakan 2929
Versi kebijakan 2929
Dokumen kebijakan JSON 2929
Pelajari selengkapnya 2930
AWSIotRoboRunnerReadOnly 2930
Menggunakan kebijakan ini 2930
Detail kebijakan 2930
Versi kebijakan 2931
Dokumen kebijakan JSON 2931
Pelajari selengkapnya 2931
AWSIotRoboRunnerServiceRolePolicy 2932
Menggunakan kebijakan ini 2932
Detail kebijakan 2932
Versi kebijakan 2932
Dokumen kebijakan JSON 2932
Pelajari selengkapnya 2933
AWSIoTRuleActions 2933
Menggunakan kebijakan ini 2933
Detail kebijakan 2933
Versi kebijakan 2933
Dokumen kebijakan JSON 2934
Pelajari selengkapnya 2934
AWSIoTSiteWiseConsoleFullAccess 2934
Menggunakan kebijakan ini 2935
Detail kebijakan 2935
Versi kebijakan 2935
Dokumen kebijakan JSON 2935
Pelajari selengkapnya 2937

AWSIoTSiteWiseFullAccess 2937
Menggunakan kebijakan ini 2938
Detail kebijakan 2938
Versi kebijakan 2938
Dokumen kebijakan JSON 2938
Pelajari selengkapnya 2938
AWSIoTSiteWiseMonitorPortalAccess 2939
Menggunakan kebijakan ini 2939
Detail kebijakan 2939
Versi kebijakan 2939
Dokumen kebijakan JSON 2939
Pelajari selengkapnya 2940
AWSIoTSiteWiseMonitorServiceRolePolicy 2941
Menggunakan kebijakan ini 2941
Detail kebijakan 2941
Versi kebijakan 2941
Dokumen kebijakan JSON 2941
Pelajari selengkapnya 2942
AWSIoTSiteWiseReadOnlyAccess 2942
Menggunakan kebijakan ini 2943
Detail kebijakan 2943
Versi kebijakan 2943
Dokumen kebijakan JSON 2943
Pelajari selengkapnya 2945
AWSIoTThingsRegistration 2945
Menggunakan kebijakan ini 2945
Detail kebijakan 2945
Versi kebijakan 2945
Dokumen kebijakan JSON 2946
Pelajari selengkapnya 2947
AWSIoTTwinMakerServiceRolePolicy 2947
Menggunakan kebijakan ini 2947
Detail kebijakan 2947
Versi kebijakan 2947
Dokumen kebijakan JSON 2948
Pelajari selengkapnya 2949

AWSIoTWirelessDataAccess 2949
Menggunakan kebijakan ini 2949
Detail kebijakan 2949
Versi kebijakan 2950
Dokumen kebijakan JSON 2950
Pelajari selengkapnya 2950
AWSIoTWirelessFullAccess 2950
Menggunakan kebijakan ini 2951
Detail kebijakan 2951
Versi kebijakan 2951
Dokumen kebijakan JSON 2951
Pelajari selengkapnya 2951
AWSIoTWirelessFullPublishAccess 2952
Menggunakan kebijakan ini 2952
Detail kebijakan 2952
Versi kebijakan 2952
Dokumen kebijakan JSON 2952
Pelajari selengkapnya 2953
AWSIoTWirelessGatewayCertManager 2953
Menggunakan kebijakan ini 2953
Detail kebijakan 2953
Versi kebijakan 2953
Dokumen kebijakan JSON 2954
Pelajari selengkapnya 2954
AWSIoTWirelessLogging 2954
Menggunakan kebijakan ini 2954
Detail kebijakan 2955
Versi kebijakan 2955
Dokumen kebijakan JSON 2955
Pelajari selengkapnya 2955
AWSIoTWirelessReadOnlyAccess 2956
Menggunakan kebijakan ini 2956
Detail kebijakan 2956
Versi kebijakan 2956
Dokumen kebijakan JSON 2956
Pelajari selengkapnya 2957

AWSIPAMServiceRolePolicy 2957
Menggunakan kebijakan ini 2957
Detail kebijakan 2957
Versi kebijakan 2957
Dokumen kebijakan JSON 2958
Pelajari selengkapnya 2960
AWSIQContractServiceRolePolicy 2960
Menggunakan kebijakan ini 2960
Detail kebijakan 2960
Versi kebijakan 2960
Dokumen kebijakan JSON 2960
Pelajari selengkapnya 2961
AWSIQFullAccess 2961
Menggunakan kebijakan ini 2961
Detail kebijakan 2961
Versi kebijakan 2961
Dokumen kebijakan JSON 2962
Pelajari selengkapnya 2962
AWSIQPermissionServiceRolePolicy 2963
Menggunakan kebijakan ini 2963
Detail kebijakan 2963
Versi kebijakan 2963
Dokumen kebijakan JSON 2963
Pelajari selengkapnya 2964
AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy 2964
Menggunakan kebijakan ini 2964
Detail kebijakan 2965
Versi kebijakan 2965
Dokumen kebijakan JSON 2965
Pelajari selengkapnya 2966
AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy 2966
Menggunakan kebijakan ini 2966
Detail kebijakan 2966
Versi kebijakan 2966
Dokumen kebijakan JSON 2966
Pelajari selengkapnya 2967

AWSKeyManagementServicePowerUser 2967
Menggunakan kebijakan ini 2967
Detail kebijakan 2967
Versi kebijakan 2967
Dokumen kebijakan JSON 2968
Pelajari selengkapnya 2968
AWSLakeFormationCrossAccountManager 2969
Menggunakan kebijakan ini 2969
Detail kebijakan 2969
Versi kebijakan 2969
Dokumen kebijakan JSON 2969
Pelajari selengkapnya 2971
AWSLakeFormationDataAdmin 2971
Menggunakan kebijakan ini 2972
Detail kebijakan 2972
Versi kebijakan 2972
Dokumen kebijakan JSON 2972
Pelajari selengkapnya 2973
AWSLambda_FullAccess 2974
Menggunakan kebijakan ini 2974
Detail kebijakan 2974
Versi kebijakan 2974
Dokumen kebijakan JSON 2974
Pelajari selengkapnya 2976
AWSLambda_ReadOnlyAccess 2976
Menggunakan kebijakan ini 2976
Detail kebijakan 2976
Versi kebijakan 2977
Dokumen kebijakan JSON 2977
Pelajari selengkapnya 2978
AWSLambdaBasicDurableExecutionRolePolicy 2978
Menggunakan kebijakan ini 2978
Detail kebijakan 2979
Versi kebijakan 2979
Dokumen kebijakan JSON 2979
Pelajari selengkapnya 2979

AWSLambdaBasicExecutionRole 2980
Menggunakan kebijakan ini 2980
Detail kebijakan 2980
Versi kebijakan 2980
Dokumen kebijakan JSON 2980
Pelajari selengkapnya 2981
AWSLambdaDynamoDBExecutionRole 2981
Menggunakan kebijakan ini 2981
Detail kebijakan 2981
Versi kebijakan 2981
Dokumen kebijakan JSON 2982
Pelajari selengkapnya 2982
AWSLambdaENIManagementAccess 2982
Menggunakan kebijakan ini 2983
Detail kebijakan 2983
Versi kebijakan 2983
Dokumen kebijakan JSON 2983
Pelajari selengkapnya 2984
AWSLambdaExecute 2984
Menggunakan kebijakan ini 2984
Detail kebijakan 2984
Versi kebijakan 2985
Dokumen kebijakan JSON 2985
Pelajari selengkapnya 2985
AWSLambdaFullAccess 2986
Menggunakan kebijakan ini 2986
Detail kebijakan 2986
Versi kebijakan 2986
Dokumen kebijakan JSON 2986
Pelajari selengkapnya 2988
AWSLambdaInvocation-DynamoDB 2988
Menggunakan kebijakan ini 2988
Detail kebijakan 2988
Versi kebijakan 2988
Dokumen kebijakan JSON 2989
Pelajari selengkapnya 2989

AWSLambdaInvokeWebFunctionEndpointAccess 2989
Menggunakan kebijakan ini 2990
Detail kebijakan 2990
Versi kebijakan 2990
Dokumen kebijakan JSON 2990
Pelajari selengkapnya 2991
AWSLambdaKinesisExecutionRole 2991
Menggunakan kebijakan ini 2991
Detail kebijakan 2991
Versi kebijakan 2991
Dokumen kebijakan JSON 2991
Pelajari selengkapnya 2992
AWSLambdaManagedEC2ResourceOperator 2992
Menggunakan kebijakan ini 2992
Detail kebijakan 2993
Versi kebijakan 2993
Dokumen kebijakan JSON 2993
Pelajari selengkapnya 2995
AWSLambdaMSKExecutionRole 2995
Menggunakan kebijakan ini 2995
Detail kebijakan 2995
Versi kebijakan 2996
Dokumen kebijakan JSON 2996
Pelajari selengkapnya 2996
AWSLambdaNetworkConnectorOperatorPolicy 2997
Menggunakan kebijakan ini 2997
Detail kebijakan 2997
Versi kebijakan 2997
Dokumen kebijakan JSON 2997
Pelajari selengkapnya 2998
AWSLambdaReplicator 2999
Menggunakan kebijakan ini 2999
Detail kebijakan 2999
Versi kebijakan 2999
Dokumen kebijakan JSON 2999
Pelajari selengkapnya 3000

AWSLambdaRole 3000
Menggunakan kebijakan ini 3001
Detail kebijakan 3001
Versi kebijakan 3001
Dokumen kebijakan JSON 3001
Pelajari selengkapnya 3001
AWSLambdaServiceRolePolicy 3002
Menggunakan kebijakan ini 3002
Detail kebijakan 3002
Versi kebijakan 3002
Dokumen kebijakan JSON 3002
Pelajari selengkapnya 3004
AWSLambdaSQSQueueExecutionRole 3004
Menggunakan kebijakan ini 3004
Detail kebijakan 3004
Versi kebijakan 3004
Dokumen kebijakan JSON 3004
Pelajari selengkapnya 3005
AWSLambdaVPCAccessExecutionRole 3005
Menggunakan kebijakan ini 3005
Detail kebijakan 3005
Versi kebijakan 3006
Dokumen kebijakan JSON 3006
Pelajari selengkapnya 3006
AWSLicenseManagerConsumptionPolicy 3007
Menggunakan kebijakan ini 3007
Detail kebijakan 3007
Versi kebijakan 3007
Dokumen kebijakan JSON 3007
Pelajari selengkapnya 3008
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy 3008
Menggunakan kebijakan ini 3008
Detail kebijakan 3008
Versi kebijakan 3009
Dokumen kebijakan JSON 3009
Pelajari selengkapnya 3010

AWSLicenseManagerMasterAccountRolePolicy 3011
Menggunakan kebijakan ini 3011
Detail kebijakan 3011
Versi kebijakan 3011
Dokumen kebijakan JSON 3011
Pelajari selengkapnya 3016
AWSLicenseManagerMemberAccountRolePolicy 3016
Menggunakan kebijakan ini 3016
Detail kebijakan 3016
Versi kebijakan 3017
Dokumen kebijakan JSON 3017
Pelajari selengkapnya 3018
AWSLicenseManagerServiceRolePolicy 3018
Menggunakan kebijakan ini 3018
Detail kebijakan 3018
Versi kebijakan 3019
Dokumen kebijakan JSON 3019
Pelajari selengkapnya 3022
AWSLicenseManagerUserSubscriptionsServiceRolePolicy 3023
Menggunakan kebijakan ini 3023
Detail kebijakan 3023
Versi kebijakan 3023
Dokumen kebijakan JSON 3023
Pelajari selengkapnya 3026
AWSM2ServicePolicy 3027
Menggunakan kebijakan ini 3027
Detail kebijakan 3027
Versi kebijakan 3027
Dokumen kebijakan JSON 3027
Pelajari selengkapnya 3029
AWSManagedAccountManagementAccess 3029
Menggunakan kebijakan ini 3029
Detail kebijakan 3029
Versi kebijakan 3029
Dokumen kebijakan JSON 3029
Pelajari selengkapnya 3030

AWSManagedAccountUserEntitlementAccess 3031
Menggunakan kebijakan ini 3031
Detail kebijakan 3031
Versi kebijakan 3031
Dokumen kebijakan JSON 3031
Pelajari selengkapnya 3032
AWSManagedAdvancedFeaturesActivationAccess 3032
Menggunakan kebijakan ini 3032
Detail kebijakan 3032
Versi kebijakan 3032
Dokumen kebijakan JSON 3033
Pelajari selengkapnya 3033
AWSManagedBudgetsSpendLimitManagementAccess 3033
Menggunakan kebijakan ini 3033
Detail kebijakan 3034
Versi kebijakan 3034
Dokumen kebijakan JSON 3034
Pelajari selengkapnya 3035
AWSManagedControlPolicyManagementAccess 3035
Menggunakan kebijakan ini 3035
Detail kebijakan 3036
Versi kebijakan 3036
Dokumen kebijakan JSON 3036
Pelajari selengkapnya 3037
AWSManagedServiceAccessManagementAccess 3037
Menggunakan kebijakan ini 3037
Detail kebijakan 3037
Versi kebijakan 3037
Dokumen kebijakan JSON 3038
Pelajari selengkapnya 3039
AWSManagedServices_ContactsServiceRolePolicy 3039
Menggunakan kebijakan ini 3040
Detail kebijakan 3040
Versi kebijakan 3040
Dokumen kebijakan JSON 3040
Pelajari selengkapnya 3041

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy 3041
Menggunakan kebijakan ini 3041
Detail kebijakan 3041
Versi kebijakan 3042
Dokumen kebijakan JSON 3042
Pelajari selengkapnya 3043
AWSManagedServices_EventsServiceRolePolicy 3043
Menggunakan kebijakan ini 3044
Detail kebijakan 3044
Versi kebijakan 3044
Dokumen kebijakan JSON 3044
Pelajari selengkapnya 3045
AWSManagedServices_SelfServiceReporting_ServiceRolePolicy 3045
Menggunakan kebijakan ini 3045
Detail kebijakan 3045
Versi kebijakan 3046
Dokumen kebijakan JSON 3046
Pelajari selengkapnya 3046
AWSManagedServicesDeploymentToolkitPolicy 3046
Menggunakan kebijakan ini 3047
Detail kebijakan 3047
Versi kebijakan 3047
Dokumen kebijakan JSON 3047
Pelajari selengkapnya 3049
AWSManagedSettingsAdminAccess 3049
Menggunakan kebijakan ini 3050
Detail kebijakan 3050
Versi kebijakan 3050
Dokumen kebijakan JSON 3050
Pelajari selengkapnya 3060
AWSManagedSettingsReadOnlyAccess 3061
Menggunakan kebijakan ini 3061
Detail kebijakan 3061
Versi kebijakan 3061
Dokumen kebijakan JSON 3061
Pelajari selengkapnya 3063

AWSManagedSignUpAdminAccess 3063
Menggunakan kebijakan ini 3063
Detail kebijakan 3063
Versi kebijakan 3063
Dokumen kebijakan JSON 3063
Pelajari selengkapnya 3065
AWSManagementConsoleAdministratorAccess 3065
Menggunakan kebijakan ini 3066
Detail kebijakan 3066
Versi kebijakan 3066
Dokumen kebijakan JSON 3066
Pelajari selengkapnya 3068
AWSManagementConsoleBasicUserAccess 3069
Menggunakan kebijakan ini 3069
Detail kebijakan 3069
Versi kebijakan 3069
Dokumen kebijakan JSON 3069
Pelajari selengkapnya 3070
AWSMarketplaceAmiIngestion 3071
Menggunakan kebijakan ini 3071
Detail kebijakan 3071
Versi kebijakan 3071
Dokumen kebijakan JSON 3071
Pelajari selengkapnya 3072
AWSMarketplaceDeploymentServiceRolePolicy 3072
Menggunakan kebijakan ini 3072
Detail kebijakan 3072
Versi kebijakan 3073
Dokumen kebijakan JSON 3073
Pelajari selengkapnya 3074
AWSMarketplaceDiscoveryFullAccess 3074
Menggunakan kebijakan ini 3074
Detail kebijakan 3075
Versi kebijakan 3075
Dokumen kebijakan JSON 3075
Pelajari selengkapnya 3076

AWSMarketplaceFullAccess 3076
Menggunakan kebijakan ini 3076
Detail kebijakan 3076
Versi kebijakan 3076
Dokumen kebijakan JSON 3077
Pelajari selengkapnya 3079
AWSMarketplaceGetEntitlements 3079
Menggunakan kebijakan ini 3079
Detail kebijakan 3080
Versi kebijakan 3080
Dokumen kebijakan JSON 3080
Pelajari selengkapnya 3080
AWSMarketplaceImageBuildFullAccess 3081
Menggunakan kebijakan ini 3081
Detail kebijakan 3081
Versi kebijakan 3081
Dokumen kebijakan JSON 3081
Pelajari selengkapnya 3085
AWSMarketplaceLicenseManagementServiceRolePolicy 3085
Menggunakan kebijakan ini 3085
Detail kebijakan 3085
Versi kebijakan 3086
Dokumen kebijakan JSON 3086
Pelajari selengkapnya 3086
AWSMarketplaceManageSubscriptions 3087
Menggunakan kebijakan ini 3087
Detail kebijakan 3087
Versi kebijakan 3087
Dokumen kebijakan JSON 3087
Pelajari selengkapnya 3090
AWSMarketplaceMeteringFullAccess 3091
Menggunakan kebijakan ini 3091
Detail kebijakan 3091
Versi kebijakan 3091
Dokumen kebijakan JSON 3091
Pelajari selengkapnya 3092

AWSMarketplaceMeteringRegisterUsage 3092
Menggunakan kebijakan ini 3092
Detail kebijakan 3092
Versi kebijakan 3092
Dokumen kebijakan JSON 3093
Pelajari selengkapnya 3093
AWSMarketplaceProcurementSystemAdminFullAccess 3093
Menggunakan kebijakan ini 3093
Detail kebijakan 3093
Versi kebijakan 3094
Dokumen kebijakan JSON 3094
Pelajari selengkapnya 3094
AWSMarketplacePurchaseOrdersServiceRolePolicy 3095
Menggunakan kebijakan ini 3095
Detail kebijakan 3095
Versi kebijakan 3095
Dokumen kebijakan JSON 3095
Pelajari selengkapnya 3096
AWSMarketplaceRead-only 3096
Menggunakan kebijakan ini 3096
Detail kebijakan 3096
Versi kebijakan 3096
Dokumen kebijakan JSON 3097
Pelajari selengkapnya 3099
AWSMarketplaceResaleAuthorizationServiceRolePolicy 3099
Menggunakan kebijakan ini 3099
Detail kebijakan 3099
Versi kebijakan 3099
Dokumen kebijakan JSON 3100
Pelajari selengkapnya 3102
AWSMarketplaceSellerFullAccess 3102
Menggunakan kebijakan ini 3102
Detail kebijakan 3102
Versi kebijakan 3103
Dokumen kebijakan JSON 3103
Pelajari selengkapnya 3110

AWSMarketplaceSellerOfferManagement 3110
Menggunakan kebijakan ini 3110
Detail kebijakan 3110
Versi kebijakan 3110
Dokumen kebijakan JSON 3111
Pelajari selengkapnya 3113
AWSMarketplaceSellerProductsFullAccess 3113
Menggunakan kebijakan ini 3114
Detail kebijakan 3114
Versi kebijakan 3114
Dokumen kebijakan JSON 3114
Pelajari selengkapnya 3117
AWSMarketplaceSellerProductsReadOnly 3118
Menggunakan kebijakan ini 3118
Detail kebijakan 3118
Versi kebijakan 3118
Dokumen kebijakan JSON 3118
Pelajari selengkapnya 3119
AWSMcpServiceActionsFullAccess 3119
Menggunakan kebijakan ini 3120
Detail kebijakan 3120
Versi kebijakan 3120
Dokumen kebijakan JSON 3120
Pelajari selengkapnya 3121
AWSMCPSignInOAuthAccessPolicy 3121
Menggunakan kebijakan ini 3121
Detail kebijakan 3121
Versi kebijakan 3121
Dokumen kebijakan JSON 3121
Pelajari selengkapnya 3122
AWSMediaConnectServicePolicy 3122
Menggunakan kebijakan ini 3122
Detail kebijakan 3122
Versi kebijakan 3123
Dokumen kebijakan JSON 3123
Pelajari selengkapnya 3125

AWSMediaLiveAnywhereServiceRolePolicy 3125
Menggunakan kebijakan ini 3125
Detail kebijakan 3125
Versi kebijakan 3125
Dokumen kebijakan JSON 3125
Pelajari selengkapnya 3128
AWSMediaTailorServiceRolePolicy 3129
Menggunakan kebijakan ini 3129
Detail kebijakan 3129
Versi kebijakan 3129
Dokumen kebijakan JSON 3129
Pelajari selengkapnya 3130
AWSMigrationHubDiscoveryAccess 3130
Menggunakan kebijakan ini 3130
Detail kebijakan 3130
Versi kebijakan 3130
Dokumen kebijakan JSON 3131
Pelajari selengkapnya 3132
AWSMigrationHubDMSAccess 3132
Menggunakan kebijakan ini 3132
Detail kebijakan 3132
Versi kebijakan 3133
Dokumen kebijakan JSON 3133
Pelajari selengkapnya 3134
AWSMigrationHubFullAccess 3134
Menggunakan kebijakan ini 3134
Detail kebijakan 3134
Versi kebijakan 3134
Dokumen kebijakan JSON 3135
Pelajari selengkapnya 3136
AWSMigrationHubOrchestratorConsoleFullAccess 3136
Menggunakan kebijakan ini 3136
Detail kebijakan 3136
Versi kebijakan 3137
Dokumen kebijakan JSON 3137
Pelajari selengkapnya 3140

AWSMigrationHubOrchestratorInstanceRolePolicy 3140
Menggunakan kebijakan ini 3140
Detail kebijakan 3140
Versi kebijakan 3141
Dokumen kebijakan JSON 3141
Pelajari selengkapnya 3141
AWSMigrationHubOrchestratorPlugin 3142
Menggunakan kebijakan ini 3142
Detail kebijakan 3142
Versi kebijakan 3142
Dokumen kebijakan JSON 3142
Pelajari selengkapnya 3144
AWSMigrationHubOrchestratorServiceRolePolicy 3144
Menggunakan kebijakan ini 3144
Detail kebijakan 3144
Versi kebijakan 3144
Dokumen kebijakan JSON 3145
Pelajari selengkapnya 3148
AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess 3148
Menggunakan kebijakan ini 3149
Detail kebijakan 3149
Versi kebijakan 3149
Dokumen kebijakan JSON 3149
Pelajari selengkapnya 3155
AWSMigrationHubRefactorSpaces-SSMAutomationPolicy 3155
Menggunakan kebijakan ini 3155
Detail kebijakan 3155
Versi kebijakan 3156
Dokumen kebijakan JSON 3156
Pelajari selengkapnya 3157
AWSMigrationHubRefactorSpacesFullAccess 3157
Menggunakan kebijakan ini 3158
Detail kebijakan 3158
Versi kebijakan 3158
Dokumen kebijakan JSON 3158
Pelajari selengkapnya 3165

AWSMigrationHubRefactorSpacesServiceRolePolicy 3165
Menggunakan kebijakan ini 3165
Detail kebijakan 3165
Versi kebijakan 3165
Dokumen kebijakan JSON 3166
Pelajari selengkapnya 3169
AWSMigrationHubSMSAccess 3169
Menggunakan kebijakan ini 3170
Detail kebijakan 3170
Versi kebijakan 3170
Dokumen kebijakan JSON 3170
Pelajari selengkapnya 3171
AWSMigrationHubStrategyCollector 3171
Menggunakan kebijakan ini 3171
Detail kebijakan 3172
Versi kebijakan 3172
Dokumen kebijakan JSON 3172
Pelajari selengkapnya 3174
AWSMigrationHubStrategyConsoleFullAccess 3174
Menggunakan kebijakan ini 3175
Detail kebijakan 3175
Versi kebijakan 3175
Dokumen kebijakan JSON 3175
Pelajari selengkapnya 3177
AWSMigrationHubStrategyServiceRolePolicy 3177
Menggunakan kebijakan ini 3177
Detail kebijakan 3177
Versi kebijakan 3178
Dokumen kebijakan JSON 3178
Pelajari selengkapnya 3179
AWSMobileHub_FullAccess 3179
Menggunakan kebijakan ini 3179
Detail kebijakan 3179
Versi kebijakan 3179
Dokumen kebijakan JSON 3180
Pelajari selengkapnya 3181

AWSMobileHub_ReadOnly 3181
Menggunakan kebijakan ini 3181
Detail kebijakan 3182
Versi kebijakan 3182
Dokumen kebijakan JSON 3182
Pelajari selengkapnya 3183
AWSMSKReplicatorExecutionRole 3183
Menggunakan kebijakan ini 3184
Detail kebijakan 3184
Versi kebijakan 3184
Dokumen kebijakan JSON 3184
Pelajari selengkapnya 3185
AWSNATGatewayServiceRolePolicy 3186
Menggunakan kebijakan ini 3186
Detail kebijakan 3186
Versi kebijakan 3186
Dokumen kebijakan JSON 3186
Pelajari selengkapnya 3187
AWSNetworkFirewallFullAccess 3187
Menggunakan kebijakan ini 3187
Detail kebijakan 3187
Versi kebijakan 3188
Dokumen kebijakan JSON 3188
Pelajari selengkapnya 3192
AWSNetworkFirewallReadOnlyAccess 3192
Menggunakan kebijakan ini 3192
Detail kebijakan 3192
Versi kebijakan 3192
Dokumen kebijakan JSON 3193
Pelajari selengkapnya 3194
AWSNetworkFirewallServiceRolePolicy 3194
Menggunakan kebijakan ini 3194
Detail kebijakan 3194
Versi kebijakan 3194
Dokumen kebijakan JSON 3195
Pelajari selengkapnya 3196

AWSNetworkManagerCloudWANServiceRolePolicy 3197
Menggunakan kebijakan ini 3197
Detail kebijakan 3197
Versi kebijakan 3197
Dokumen kebijakan JSON 3197
Pelajari selengkapnya 3198
AWSNetworkManagerFullAccess 3198
Menggunakan kebijakan ini 3198
Detail kebijakan 3198
Versi kebijakan 3198
Dokumen kebijakan JSON 3199
Pelajari selengkapnya 3199
AWSNetworkManagerReadOnlyAccess 3199
Menggunakan kebijakan ini 3200
Detail kebijakan 3200
Versi kebijakan 3200
Dokumen kebijakan JSON 3200
Pelajari selengkapnya 3201
AWSNetworkManagerServiceRolePolicy 3201
Menggunakan kebijakan ini 3201
Detail kebijakan 3201
Versi kebijakan 3201
Dokumen kebijakan JSON 3202
Pelajari selengkapnya 3203
AWSObservabilityAdminLogsCentralizationServiceRolePolicy 3203
Menggunakan kebijakan ini 3203
Detail kebijakan 3203
Versi kebijakan 3203
Dokumen kebijakan JSON 3203
Pelajari selengkapnya 3204
AWSObservabilityAdminServiceRolePolicy 3205
Menggunakan kebijakan ini 3205
Detail kebijakan 3205
Versi kebijakan 3205
Dokumen kebijakan JSON 3205
Pelajari selengkapnya 3208

AWSObservabilityAdminTelemetryEnablementServiceRolePolicy 3208
Menggunakan kebijakan ini 3208
Detail kebijakan 3208
Versi kebijakan 3209
Dokumen kebijakan JSON 3209
Pelajari selengkapnya 3226
AWSOrganizationsFullAccess 3226
Menggunakan kebijakan ini 3226
Detail kebijakan 3226
Versi kebijakan 3227
Dokumen kebijakan JSON 3227
Pelajari selengkapnya 3228
AWSOrganizationsReadOnlyAccess 3228
Menggunakan kebijakan ini 3228
Detail kebijakan 3228
Versi kebijakan 3228
Dokumen kebijakan JSON 3229
Pelajari selengkapnya 3229
AWSOrganizationsServiceTrustPolicy 3230
Menggunakan kebijakan ini 3230
Detail kebijakan 3230
Versi kebijakan 3230
Dokumen kebijakan JSON 3230
Pelajari selengkapnya 3231
AWSOutpostsAuthorizeServerPolicy 3231
Menggunakan kebijakan ini 3231
Detail kebijakan 3231
Versi kebijakan 3232
Dokumen kebijakan JSON 3232
Pelajari selengkapnya 3232
AWSOutpostsServiceRolePolicy 3233
Menggunakan kebijakan ini 3233
Detail kebijakan 3233
Versi kebijakan 3233
Dokumen kebijakan JSON 3233
Pelajari selengkapnya 3235

AWSPanoramaApplianceRolePolicy 3235
Menggunakan kebijakan ini 3235
Detail kebijakan 3235
Versi kebijakan 3236
Dokumen kebijakan JSON 3236
Pelajari selengkapnya 3236
AWSPanoramaApplianceServiceRolePolicy 3237
Menggunakan kebijakan ini 3237
Detail kebijakan 3237
Versi kebijakan 3237
Dokumen kebijakan JSON 3237
Pelajari selengkapnya 3239
AWSPanoramaFullAccess 3239
Menggunakan kebijakan ini 3239
Detail kebijakan 3239
Versi kebijakan 3239
Dokumen kebijakan JSON 3240
Pelajari selengkapnya 3242
AWSPanoramaGreengrassGroupRolePolicy 3242
Menggunakan kebijakan ini 3243
Detail kebijakan 3243
Versi kebijakan 3243
Dokumen kebijakan JSON 3243
Pelajari selengkapnya 3244
AWSPanoramaSageMakerRolePolicy 3245
Menggunakan kebijakan ini 3245
Detail kebijakan 3245
Versi kebijakan 3245
Dokumen kebijakan JSON 3245
Pelajari selengkapnya 3246
AWSPanoramaServiceLinkedRolePolicy 3246
Menggunakan kebijakan ini 3246
Detail kebijakan 3246
Versi kebijakan 3247
Dokumen kebijakan JSON 3247
Pelajari selengkapnya 3249

AWSPanoramaServiceRolePolicy 3250
Menggunakan kebijakan ini 3250
Detail kebijakan 3250
Versi kebijakan 3250
Dokumen kebijakan JSON 3250
Pelajari selengkapnya 3257
AWSPartnerCentralChannelHandshakeApprovalManagement 3257
Menggunakan kebijakan ini 3258
Detail kebijakan 3258
Versi kebijakan 3258
Dokumen kebijakan JSON 3258
Pelajari selengkapnya 3259
AWSPartnerCentralChannelManagement 3259
Menggunakan kebijakan ini 3259
Detail kebijakan 3259
Versi kebijakan 3259
Dokumen kebijakan JSON 3260
Pelajari selengkapnya 3262
AWSPartnerCentralFullAccess 3263
Menggunakan kebijakan ini 3263
Detail kebijakan 3263
Versi kebijakan 3263
Dokumen kebijakan JSON 3263
Pelajari selengkapnya 3268
AWSPartnerCentralMarketingManagement 3268
Menggunakan kebijakan ini 3268
Detail kebijakan 3268
Versi kebijakan 3268
Dokumen kebijakan JSON 3269
Pelajari selengkapnya 3271
AWSPartnerCentralOpportunityManagement 3271
Menggunakan kebijakan ini 3271
Detail kebijakan 3272
Versi kebijakan 3272
Dokumen kebijakan JSON 3272
Pelajari selengkapnya 3276

AWSPartnerCentralRevenueAttributionManagement 3276
Menggunakan kebijakan ini 3277
Detail kebijakan 3277
Versi kebijakan 3277
Dokumen kebijakan JSON 3277
Pelajari selengkapnya 3282
AWSPartnerCentralSandboxFullAccess 3282
Menggunakan kebijakan ini 3282
Detail kebijakan 3282
Versi kebijakan 3282
Dokumen kebijakan JSON 3283
Pelajari selengkapnya 3284
AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy 3284
Menggunakan kebijakan ini 3284
Detail kebijakan 3284
Versi kebijakan 3285
Dokumen kebijakan JSON 3285
Pelajari selengkapnya 3285
AWSPartnerLedSupportReadOnlyAccess 3286
Menggunakan kebijakan ini 3286
Detail kebijakan 3286
Versi kebijakan 3286
Dokumen kebijakan JSON 3286
Pelajari selengkapnya 3323
AWSPartnerProServeToolsFullAccess 3323
Menggunakan kebijakan ini 3324
Detail kebijakan 3324
Versi kebijakan 3324
Dokumen kebijakan JSON 3324
Pelajari selengkapnya 3325
AWSPartnerProServeToolsIndividualContributor 3325
Menggunakan kebijakan ini 3325
Detail kebijakan 3325
Versi kebijakan 3325
Dokumen kebijakan JSON 3326
Pelajari selengkapnya 3326

AWSPartnerProServeToolsOrganizationReaderIndividualContributor 3326
Menggunakan kebijakan ini 3327
Detail kebijakan 3327
Versi kebijakan 3327
Dokumen kebijakan JSON 3327
Pelajari selengkapnya 3328
AWSPCSComputeNodePolicy 3328
Menggunakan kebijakan ini 3328
Detail kebijakan 3328
Versi kebijakan 3328
Dokumen kebijakan JSON 3329
Pelajari selengkapnya 3329
AWSPCSServiceRolePolicy 3329
Menggunakan kebijakan ini 3329
Detail kebijakan 3329
Versi kebijakan 3330
Dokumen kebijakan JSON 3330
Pelajari selengkapnya 3335
AWSPriceListServiceFullAccess 3335
Menggunakan kebijakan ini 3335
Detail kebijakan 3335
Versi kebijakan 3335
Dokumen kebijakan JSON 3336
Pelajari selengkapnya 3336
AWSPrivateCAAuditor 3336
Menggunakan kebijakan ini 3336
Detail kebijakan 3337
Versi kebijakan 3337
Dokumen kebijakan JSON 3337
Pelajari selengkapnya 3338
AWSPrivateCAConnectorForKubernetesPolicy 3338
Menggunakan kebijakan ini 3338
Detail kebijakan 3338
Versi kebijakan 3338
Dokumen kebijakan JSON 3339
Pelajari selengkapnya 3339

AWSPrivateCAFullAccess 3339
Menggunakan kebijakan ini 3339
Detail kebijakan 3339
Versi kebijakan 3340
Dokumen kebijakan JSON 3340
Pelajari selengkapnya 3340
AWSPrivateCAPrivilegedUser 3340
Menggunakan kebijakan ini 3341
Detail kebijakan 3341
Versi kebijakan 3341
Dokumen kebijakan JSON 3341
Pelajari selengkapnya 3342
AWSPrivateCAReadOnly 3342
Menggunakan kebijakan ini 3343
Detail kebijakan 3343
Versi kebijakan 3343
Dokumen kebijakan JSON 3343
Pelajari selengkapnya 3344
AWSPrivateCAUser 3344
Menggunakan kebijakan ini 3344
Detail kebijakan 3344
Versi kebijakan 3344
Dokumen kebijakan JSON 3344
Pelajari selengkapnya 3346
AWSPrivateMarketplaceAdminFullAccess 3346
Menggunakan kebijakan ini 3346
Detail kebijakan 3346
Versi kebijakan 3346
Dokumen kebijakan JSON 3347
Pelajari selengkapnya 3349
AWSPrivateMarketplaceRequests 3349
Menggunakan kebijakan ini 3350
Detail kebijakan 3350
Versi kebijakan 3350
Dokumen kebijakan JSON 3350
Pelajari selengkapnya 3352

AWSPrivateNetworksServiceRolePolicy 3352
Menggunakan kebijakan ini 3352
Detail kebijakan 3352
Versi kebijakan 3353
Dokumen kebijakan JSON 3353
Pelajari selengkapnya 3353
AWSProtonCodeBuildProvisioningBasicAccess 3353
Menggunakan kebijakan ini 3354
Detail kebijakan 3354
Versi kebijakan 3354
Dokumen kebijakan JSON 3354
Pelajari selengkapnya 3355
AWSProtonCodeBuildProvisioningServiceRolePolicy 3355
Menggunakan kebijakan ini 3355
Detail kebijakan 3355
Versi kebijakan 3355
Dokumen kebijakan JSON 3356
Pelajari selengkapnya 3357
AWSProtonDeveloperAccess 3357
Menggunakan kebijakan ini 3357
Detail kebijakan 3357
Versi kebijakan 3358
Dokumen kebijakan JSON 3358
Pelajari selengkapnya 3360
AWSProtonFullAccess 3360
Menggunakan kebijakan ini 3360
Detail kebijakan 3361
Versi kebijakan 3361
Dokumen kebijakan JSON 3361
Pelajari selengkapnya 3363
AWSProtonReadOnlyAccess 3363
Menggunakan kebijakan ini 3363
Detail kebijakan 3363
Versi kebijakan 3364
Dokumen kebijakan JSON 3364
Pelajari selengkapnya 3365

AWSProtonServiceGitSyncServiceRolePolicy 3366
Menggunakan kebijakan ini 3366
Detail kebijakan 3366
Versi kebijakan 3366
Dokumen kebijakan JSON 3366
Pelajari selengkapnya 3367
AWSProtonSyncServiceRolePolicy 3367
Menggunakan kebijakan ini 3367
Detail kebijakan 3367
Versi kebijakan 3368
Dokumen kebijakan JSON 3368
Pelajari selengkapnya 3369
AWSPurchaseOrdersServiceRolePolicy 3369
Menggunakan kebijakan ini 3369
Detail kebijakan 3369
Versi kebijakan 3370
Dokumen kebijakan JSON 3370
Pelajari selengkapnya 3371
AWSQuickSetupCFGCPacksPermissionsBoundary 3371
Menggunakan kebijakan ini 3371
Detail kebijakan 3371
Versi kebijakan 3371
Dokumen kebijakan JSON 3372
Pelajari selengkapnya 3374
AWSQuickSetupDeploymentRolePolicy 3375
Menggunakan kebijakan ini 3375
Detail kebijakan 3375
Versi kebijakan 3375
Dokumen kebijakan JSON 3375
Pelajari selengkapnya 3384
AWSQuickSetupDevOpsGuruPermissionsBoundary 3384
Menggunakan kebijakan ini 3384
Detail kebijakan 3385
Versi kebijakan 3385
Dokumen kebijakan JSON 3385
Pelajari selengkapnya 3388

AWSQuickSetupDistributorPermissionsBoundary 3388
Menggunakan kebijakan ini 3388
Detail kebijakan 3388
Versi kebijakan 3388
Dokumen kebijakan JSON 3389
Pelajari selengkapnya 3394
AWSQuickSetupEnableAREXExecutionPolicy 3395
Menggunakan kebijakan ini 3395
Detail kebijakan 3395
Versi kebijakan 3395
Dokumen kebijakan JSON 3395
Pelajari selengkapnya 3397
AWSQuickSetupEnableDHMCExecutionPolicy 3397
Menggunakan kebijakan ini 3397
Detail kebijakan 3397
Versi kebijakan 3398
Dokumen kebijakan JSON 3398
Pelajari selengkapnya 3399
AWSQuickSetupJITNADeploymentRolePolicy 3399
Menggunakan kebijakan ini 3399
Detail kebijakan 3399
Versi kebijakan 3400
Dokumen kebijakan JSON 3400
Pelajari selengkapnya 3404
AWSQuickSetupManagedInstanceProfileExecutionPolicy 3404
Menggunakan kebijakan ini 3404
Detail kebijakan 3404
Versi kebijakan 3404
Dokumen kebijakan JSON 3405
Pelajari selengkapnya 3409
AWSQuickSetupManageJITNAResourcesExecutionPolicy 3410
Menggunakan kebijakan ini 3410
Detail kebijakan 3410
Versi kebijakan 3410
Dokumen kebijakan JSON 3410
Pelajari selengkapnya 3412

AWSQuickSetupPatchPolicyBaselineAccess 3413
Menggunakan kebijakan ini 3413
Detail kebijakan 3413
Versi kebijakan 3413
Dokumen kebijakan JSON 3413
Pelajari selengkapnya 3414
AWSQuickSetupPatchPolicyDeploymentRolePolicy 3414
Menggunakan kebijakan ini 3415
Detail kebijakan 3415
Versi kebijakan 3415
Dokumen kebijakan JSON 3415
Pelajari selengkapnya 3423
AWSQuickSetupPatchPolicyLambdaExecutionPolicy 3424
Menggunakan kebijakan ini 3424
Detail kebijakan 3424
Versi kebijakan 3424
Dokumen kebijakan JSON 3424
Pelajari selengkapnya 3425
AWSQuickSetupPatchPolicyPermissionsBoundary 3425
Menggunakan kebijakan ini 3426
Detail kebijakan 3426
Versi kebijakan 3426
Dokumen kebijakan JSON 3426
Pelajari selengkapnya 3434
AWSQuickSetupPatchPolicyTagManagementExecutionPolicy 3435
Menggunakan kebijakan ini 3435
Detail kebijakan 3435
Versi kebijakan 3435
Dokumen kebijakan JSON 3435
Pelajari selengkapnya 3436
AWSQuickSetupSchedulerPermissionsBoundary 3437
Menggunakan kebijakan ini 3437
Detail kebijakan 3437
Versi kebijakan 3437
Dokumen kebijakan JSON 3437
Pelajari selengkapnya 3441

AWSQuickSetupSSMDeploymentRolePolicy 3441
Menggunakan kebijakan ini 3441
Detail kebijakan 3441
Versi kebijakan 3441
Dokumen kebijakan JSON 3441
Pelajari selengkapnya 3453
AWSQuickSetupSSMDeploymentS3BucketRolePolicy 3453
Menggunakan kebijakan ini 3453
Detail kebijakan 3453
Versi kebijakan 3453
Dokumen kebijakan JSON 3454
Pelajari selengkapnya 3454
AWSQuickSetupSSMHostMgmtPermissionsBoundary 3455
Menggunakan kebijakan ini 3455
Detail kebijakan 3455
Versi kebijakan 3455
Dokumen kebijakan JSON 3455
Pelajari selengkapnya 3461
AWSQuickSetupSSMLifecycleManagementExecutionPolicy 3461
Menggunakan kebijakan ini 3462
Detail kebijakan 3462
Versi kebijakan 3462
Dokumen kebijakan JSON 3462
Pelajari selengkapnya 3463
AWSQuickSetupSSMManageResourcesExecutionPolicy 3464
Menggunakan kebijakan ini 3464
Detail kebijakan 3464
Versi kebijakan 3464
Dokumen kebijakan JSON 3464
Pelajari selengkapnya 3467
AWSQuickSetupStartSSMAssociationsExecutionPolicy 3467
Menggunakan kebijakan ini 3467
Detail kebijakan 3468
Versi kebijakan 3468
Dokumen kebijakan JSON 3468
Pelajari selengkapnya 3469

AWSQuickSetupStartStopInstancesExecutionPolicy 3469
Menggunakan kebijakan ini 3469
Detail kebijakan 3470
Versi kebijakan 3470
Dokumen kebijakan JSON 3470
Pelajari selengkapnya 3472
AWSQuickSightAssetBundleExportPolicy 3472
Menggunakan kebijakan ini 3472
Detail kebijakan 3472
Versi kebijakan 3472
Dokumen kebijakan JSON 3472
Pelajari selengkapnya 3475
AWSQuickSightAssetBundleImportPolicy 3475
Menggunakan kebijakan ini 3475
Detail kebijakan 3475
Versi kebijakan 3475
Dokumen kebijakan JSON 3475
Pelajari selengkapnya 3478
AWSQuicksightAthenaAccess 3479
Menggunakan kebijakan ini 3479
Detail kebijakan 3479
Versi kebijakan 3479
Dokumen kebijakan JSON 3479
Pelajari selengkapnya 3481
AWSQuickSightDescribeRDS 3482
Menggunakan kebijakan ini 3482
Detail kebijakan 3482
Versi kebijakan 3482
Dokumen kebijakan JSON 3482
Pelajari selengkapnya 3483
AWSQuickSightDescribeRedshift 3483
Menggunakan kebijakan ini 3483
Detail kebijakan 3483
Versi kebijakan 3483
Dokumen kebijakan JSON 3484
Pelajari selengkapnya 3484

AWSQuickSightElasticsearchPolicy 3484
Menggunakan kebijakan ini 3484
Detail kebijakan 3484
Versi kebijakan 3485
Dokumen kebijakan JSON 3485
Pelajari selengkapnya 3486
AWSQuickSightIoTAnalyticsAccess 3486
Menggunakan kebijakan ini 3486
Detail kebijakan 3486
Versi kebijakan 3487
Dokumen kebijakan JSON 3487
Pelajari selengkapnya 3487
AWSQuickSightListIAM 3487
Menggunakan kebijakan ini 3488
Detail kebijakan 3488
Versi kebijakan 3488
Dokumen kebijakan JSON 3488
Pelajari selengkapnya 3488
AWSQuicksightOpenSearchPolicy 3489
Menggunakan kebijakan ini 3489
Detail kebijakan 3489
Versi kebijakan 3489
Dokumen kebijakan JSON 3489
Pelajari selengkapnya 3490
AWSQuickSightSageMakerPolicy 3491
Menggunakan kebijakan ini 3491
Detail kebijakan 3491
Versi kebijakan 3491
Dokumen kebijakan JSON 3491
Pelajari selengkapnya 3492
AWSQuickSightSecretsManagerWriteAccess 3493
Menggunakan kebijakan ini 3493
Detail kebijakan 3493
Versi kebijakan 3493
Dokumen kebijakan JSON 3493
Pelajari selengkapnya 3494

AWSQuickSightSecretsManagerWritePolicy 3494
Menggunakan kebijakan ini 3495
Detail kebijakan 3495
Versi kebijakan 3495
Dokumen kebijakan JSON 3495
Pelajari selengkapnya 3496
AWSQuickSightTimestreamPolicy 3496
Menggunakan kebijakan ini 3496
Detail kebijakan 3496
Versi kebijakan 3497
Dokumen kebijakan JSON 3497
Pelajari selengkapnya 3497
AWSReachabilityAnalyzerServiceRolePolicy 3498
Menggunakan kebijakan ini 3498
Detail kebijakan 3498
Versi kebijakan 3498
Dokumen kebijakan JSON 3498
Pelajari selengkapnya 3501
AWSRefactoringToolkitFullAccess 3501
Menggunakan kebijakan ini 3501
Detail kebijakan 3501
Versi kebijakan 3501
Dokumen kebijakan JSON 3502
Pelajari selengkapnya 3515
AWSRefactoringToolkitSidecarPolicy 3515
Menggunakan kebijakan ini 3516
Detail kebijakan 3516
Versi kebijakan 3516
Dokumen kebijakan JSON 3516
Pelajari selengkapnya 3517
AWSrePostPrivateCloudWatchAccess 3517
Menggunakan kebijakan ini 3517
Detail kebijakan 3518
Versi kebijakan 3518
Dokumen kebijakan JSON 3518
Pelajari selengkapnya 3519

AWSRepostSpaceSupportOperationsPolicy 3519
Menggunakan kebijakan ini 3519
Detail kebijakan 3519
Versi kebijakan 3519
Dokumen kebijakan JSON 3519
Pelajari selengkapnya 3520
AWSResilienceHubAsssessmentExecutionPolicy 3520
Menggunakan kebijakan ini 3520
Detail kebijakan 3520
Versi kebijakan 3521
Dokumen kebijakan JSON 3521
Pelajari selengkapnya 3526
AWSResilienceHubResilienceTestingPolicy 3526
Menggunakan kebijakan ini 3526
Detail kebijakan 3526
Versi kebijakan 3526
Dokumen kebijakan JSON 3526
Pelajari selengkapnya 3529
AWSResilienceHubServiceRolePolicy 3530
Menggunakan kebijakan ini 3530
Detail kebijakan 3530
Versi kebijakan 3530
Dokumen kebijakan JSON 3530
Pelajari selengkapnya 3531
AWSResilienceHubV2AssessmentExecutionPolicy 3531
Menggunakan kebijakan ini 3531
Detail kebijakan 3531
Versi kebijakan 3532
Dokumen kebijakan JSON 3532
Pelajari selengkapnya 3538
AWSResourceAccessManagerFullAccess 3538
Menggunakan kebijakan ini 3538
Detail kebijakan 3538
Versi kebijakan 3538
Dokumen kebijakan JSON 3539
Pelajari selengkapnya 3539

AWSResourceAccessManagerReadOnlyAccess 3539
Menggunakan kebijakan ini 3539
Detail kebijakan 3539
Versi kebijakan 3540
Dokumen kebijakan JSON 3540
Pelajari selengkapnya 3540
AWSResourceAccessManagerResourceShareParticipantAccess 3540
Menggunakan kebijakan ini 3541
Detail kebijakan 3541
Versi kebijakan 3541
Dokumen kebijakan JSON 3541
Pelajari selengkapnya 3542
AWSResourceAccessManagerServiceRolePolicy 3542
Menggunakan kebijakan ini 3542
Detail kebijakan 3542
Versi kebijakan 3542
Dokumen kebijakan JSON 3543
Pelajari selengkapnya 3543
AWSResourceExplorerFullAccess 3544
Menggunakan kebijakan ini 3544
Detail kebijakan 3544
Versi kebijakan 3544
Dokumen kebijakan JSON 3544
Pelajari selengkapnya 3545
AWSResourceExplorerOrganizationsAccess 3545
Menggunakan kebijakan ini 3546
Detail kebijakan 3546
Versi kebijakan 3546
Dokumen kebijakan JSON 3546
Pelajari selengkapnya 3548
AWSResourceExplorerReadOnlyAccess 3548
Menggunakan kebijakan ini 3548
Detail kebijakan 3548
Versi kebijakan 3548
Dokumen kebijakan JSON 3549
Pelajari selengkapnya 3549

AWSResourceExplorerServiceRolePolicy 3549
Menggunakan kebijakan ini 3550
Detail kebijakan 3550
Versi kebijakan 3550
Dokumen kebijakan JSON 3550
Pelajari selengkapnya 3616
AWSResourceGroupsReadOnlyAccess 3616
Menggunakan kebijakan ini 3616
Detail kebijakan 3616
Versi kebijakan 3617
Dokumen kebijakan JSON 3617
Pelajari selengkapnya 3618
AWSRevenueAttributionManagement 3618
Menggunakan kebijakan ini 3619
Detail kebijakan 3619
Versi kebijakan 3619
Dokumen kebijakan JSON 3619
Pelajari selengkapnya 3621
AWSRoboMaker_FullAccess 3621
Menggunakan kebijakan ini 3621
Detail kebijakan 3621
Versi kebijakan 3622
Dokumen kebijakan JSON 3622
Pelajari selengkapnya 3623
AWSRoboMakerReadOnlyAccess 3623
Menggunakan kebijakan ini 3623
Detail kebijakan 3623
Versi kebijakan 3624
Dokumen kebijakan JSON 3624
Pelajari selengkapnya 3624
AWSRoboMakerServicePolicy 3625
Menggunakan kebijakan ini 3625
Detail kebijakan 3625
Versi kebijakan 3625
Dokumen kebijakan JSON 3625
Pelajari selengkapnya 3627

AWSRoboMakerServiceRolePolicy 3627
Menggunakan kebijakan ini 3627
Detail kebijakan 3627
Versi kebijakan 3627
Dokumen kebijakan JSON 3628
Pelajari selengkapnya 3629
AWSRolesAnywhereFullAccess 3629
Menggunakan kebijakan ini 3629
Detail kebijakan 3629
Versi kebijakan 3630
Dokumen kebijakan JSON 3630
Pelajari selengkapnya 3632
AWSRolesAnywhereReadOnly 3632
Menggunakan kebijakan ini 3633
Detail kebijakan 3633
Versi kebijakan 3633
Dokumen kebijakan JSON 3633
Pelajari selengkapnya 3635
AWSRolesAnywhereServicePolicy 3635
Menggunakan kebijakan ini 3635
Detail kebijakan 3635
Versi kebijakan 3635
Dokumen kebijakan JSON 3636
Pelajari selengkapnya 3636
AWSS3OnOutpostsServiceRolePolicy 3636
Menggunakan kebijakan ini 3637
Detail kebijakan 3637
Versi kebijakan 3637
Dokumen kebijakan JSON 3637
Pelajari selengkapnya 3640
AWSSavingsPlansFullAccess 3640
Menggunakan kebijakan ini 3640
Detail kebijakan 3640
Versi kebijakan 3640
Dokumen kebijakan JSON 3641
Pelajari selengkapnya 3641

AWSSavingsPlansReadOnlyAccess 3641
Menggunakan kebijakan ini 3641
Detail kebijakan 3641
Versi kebijakan 3642
Dokumen kebijakan JSON 3642
Pelajari selengkapnya 3642
AWSSDMPServiceRolePolicy 3642
Menggunakan kebijakan ini 3643
Detail kebijakan 3643
Versi kebijakan 3643
Dokumen kebijakan JSON 3643
Pelajari selengkapnya 3646
AWSSecretsManagerClientReadOnlyAccess 3646
Menggunakan kebijakan ini 3646
Detail kebijakan 3647
Versi kebijakan 3647
Dokumen kebijakan JSON 3647
Pelajari selengkapnya 3648
AWSSecurityAgentServiceRolePolicy 3648
Menggunakan kebijakan ini 3648
Detail kebijakan 3648
Versi kebijakan 3649
Dokumen kebijakan JSON 3649
Pelajari selengkapnya 3651
AWSSecurityAgentWebAppPolicy 3651
Menggunakan kebijakan ini 3651
Detail kebijakan 3651
Versi kebijakan 3651
Dokumen kebijakan JSON 3652
Pelajari selengkapnya 3654
AWSSecurityHubFullAccess 3654
Menggunakan kebijakan ini 3654
Detail kebijakan 3654
Versi kebijakan 3655
Dokumen kebijakan JSON 3655
Pelajari selengkapnya 3656

AWSSecurityHubOrganizationsAccess 3656
Menggunakan kebijakan ini 3657
Detail kebijakan 3657
Versi kebijakan 3657
Dokumen kebijakan JSON 3657
Pelajari selengkapnya 3660
AWSSecurityHubReadOnlyAccess 3660
Menggunakan kebijakan ini 3660
Detail kebijakan 3660
Versi kebijakan 3660
Dokumen kebijakan JSON 3660
Pelajari selengkapnya 3661
AWSSecurityHubServiceRolePolicy 3661
Menggunakan kebijakan ini 3661
Detail kebijakan 3661
Versi kebijakan 3662
Dokumen kebijakan JSON 3662
Pelajari selengkapnya 3665
AWSSecurityHubV2ServiceRolePolicy 3665
Menggunakan kebijakan ini 3665
Detail kebijakan 3665
Versi kebijakan 3666
Dokumen kebijakan JSON 3666
Pelajari selengkapnya 3672
AWSSecurityIncidentResponseCaseFullAccess 3672
Menggunakan kebijakan ini 3672
Detail kebijakan 3672
Versi kebijakan 3672
Dokumen kebijakan JSON 3672
Pelajari selengkapnya 3673
AWSSecurityIncidentResponseFullAccess 3674
Menggunakan kebijakan ini 3674
Detail kebijakan 3674
Versi kebijakan 3674
Dokumen kebijakan JSON 3674
Pelajari selengkapnya 3676

AWSSecurityIncidentResponseReadOnlyAccess 3676
Menggunakan kebijakan ini 3676
Detail kebijakan 3676
Versi kebijakan 3677
Dokumen kebijakan JSON 3677
Pelajari selengkapnya 3677
AWSSecurityIncidentResponseServiceRolePolicy 3678
Menggunakan kebijakan ini 3678
Detail kebijakan 3678
Versi kebijakan 3678
Dokumen kebijakan JSON 3678
Pelajari selengkapnya 3680
AWSSecurityIncidentResponseTriageServiceRolePolicy 3680
Menggunakan kebijakan ini 3680
Detail kebijakan 3680
Versi kebijakan 3680
Dokumen kebijakan JSON 3681
Pelajari selengkapnya 3683
AWSServiceCatalogAdminFullAccess 3683
Menggunakan kebijakan ini 3683
Detail kebijakan 3683
Versi kebijakan 3683
Dokumen kebijakan JSON 3684
Pelajari selengkapnya 3686
AWSServiceCatalogAdminReadOnlyAccess 3687
Menggunakan kebijakan ini 3687
Detail kebijakan 3687
Versi kebijakan 3687
Dokumen kebijakan JSON 3687
Pelajari selengkapnya 3688
AWSServiceCatalogAppRegistryFullAccess 3689
Menggunakan kebijakan ini 3689
Detail kebijakan 3689
Versi kebijakan 3689
Dokumen kebijakan JSON 3689
Pelajari selengkapnya 3692

AWSServiceCatalogAppRegistryReadOnlyAccess 3692
Menggunakan kebijakan ini 3692
Detail kebijakan 3692
Versi kebijakan 3693
Dokumen kebijakan JSON 3693
Pelajari selengkapnya 3693
AWSServiceCatalogAppRegistryServiceRolePolicy 3694
Menggunakan kebijakan ini 3694
Detail kebijakan 3694
Versi kebijakan 3694
Dokumen kebijakan JSON 3694
Pelajari selengkapnya 3696
AWSServiceCatalogEndUserFullAccess 3696
Menggunakan kebijakan ini 3696
Detail kebijakan 3696
Versi kebijakan 3696
Dokumen kebijakan JSON 3696
Pelajari selengkapnya 3698
AWSServiceCatalogEndUserReadOnlyAccess 3699
Menggunakan kebijakan ini 3699
Detail kebijakan 3699
Versi kebijakan 3699
Dokumen kebijakan JSON 3699
Pelajari selengkapnya 3701
AWSServiceCatalogOrgsDataSyncServiceRolePolicy 3701
Menggunakan kebijakan ini 3701
Detail kebijakan 3701
Versi kebijakan 3702
Dokumen kebijakan JSON 3702
Pelajari selengkapnya 3703
AWSServiceCatalogSyncServiceRolePolicy 3703
Menggunakan kebijakan ini 3703
Detail kebijakan 3703
Versi kebijakan 3703
Dokumen kebijakan JSON 3704
Pelajari selengkapnya 3705

AWSServiceRoleForAIDevOpsPolicy 3705
Menggunakan kebijakan ini 3705
Detail kebijakan 3705
Versi kebijakan 3705
Dokumen kebijakan JSON 3705
Pelajari selengkapnya 3708
AWSServiceRoleForAmazonEKSNodegroup 3708
Menggunakan kebijakan ini 3708
Detail kebijakan 3708
Versi kebijakan 3708
Dokumen kebijakan JSON 3709
Pelajari selengkapnya 3714
AWSServiceRoleForAmazonQDeveloper 3714
Menggunakan kebijakan ini 3714
Detail kebijakan 3715
Versi kebijakan 3715
Dokumen kebijakan JSON 3715
Pelajari selengkapnya 3716
AWSServiceRoleForAWSTransform 3716
Menggunakan kebijakan ini 3716
Detail kebijakan 3716
Versi kebijakan 3716
Dokumen kebijakan JSON 3717
Pelajari selengkapnya 3719
AWSServiceRoleForAWSTransformCustom 3719
Menggunakan kebijakan ini 3719
Detail kebijakan 3719
Versi kebijakan 3720
Dokumen kebijakan JSON 3720
Pelajari selengkapnya 3721
AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy 3721
Menggunakan kebijakan ini 3721
Detail kebijakan 3721
Versi kebijakan 3721
Dokumen kebijakan JSON 3722
Pelajari selengkapnya 3722

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy 3722
Menggunakan kebijakan ini 3722
Detail kebijakan 3722
Versi kebijakan 3723
Dokumen kebijakan JSON 3723
Pelajari selengkapnya 3723
AWSServiceRoleForCodeGuru-Profiler 3724
Menggunakan kebijakan ini 3724
Detail kebijakan 3724
Versi kebijakan 3724
Dokumen kebijakan JSON 3724
Pelajari selengkapnya 3725
AWSServiceRoleForCodeWhispererPolicy 3725
Menggunakan kebijakan ini 3725
Detail kebijakan 3725
Versi kebijakan 3725
Dokumen kebijakan JSON 3726
Pelajari selengkapnya 3728
AWSServiceRoleForEC2ScheduledInstances 3728
Menggunakan kebijakan ini 3728
Detail kebijakan 3729
Versi kebijakan 3729
Dokumen kebijakan JSON 3729
Pelajari selengkapnya 3730
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy 3730
Menggunakan kebijakan ini 3730
Detail kebijakan 3730
Versi kebijakan 3731
Dokumen kebijakan JSON 3731
Pelajari selengkapnya 3731
AWSServiceRoleForImageBuilder 3731
Menggunakan kebijakan ini 3731
Detail kebijakan 3732
Versi kebijakan 3732
Dokumen kebijakan JSON 3732
Pelajari selengkapnya 3743

AWSServiceRoleForIoTSiteWise 3743
Menggunakan kebijakan ini 3743
Detail kebijakan 3744
Versi kebijakan 3744
Dokumen kebijakan JSON 3744
Pelajari selengkapnya 3745
AWSServiceRoleForLogDeliveryPolicy 3745
Menggunakan kebijakan ini 3746
Detail kebijakan 3746
Versi kebijakan 3746
Dokumen kebijakan JSON 3746
Pelajari selengkapnya 3747
AWSServiceRoleForMonitronPolicy 3747
Menggunakan kebijakan ini 3747
Detail kebijakan 3747
Versi kebijakan 3748
Dokumen kebijakan JSON 3748
Pelajari selengkapnya 3749
AWSServiceRoleForNeptuneGraphPolicy 3749
Menggunakan kebijakan ini 3750
Detail kebijakan 3750
Versi kebijakan 3750
Dokumen kebijakan JSON 3750
Pelajari selengkapnya 3751
AWSServiceRoleForPrivateMarketplaceAdminPolicy 3752
Menggunakan kebijakan ini 3752
Detail kebijakan 3752
Versi kebijakan 3752
Dokumen kebijakan JSON 3752
Pelajari selengkapnya 3754
AWSServiceRoleForProcurementInsightsPolicy 3754
Menggunakan kebijakan ini 3754
Detail kebijakan 3754
Versi kebijakan 3755
Dokumen kebijakan JSON 3755
Pelajari selengkapnya 3755

AWSServiceRoleForSMS 3755
Menggunakan kebijakan ini 3756
Detail kebijakan 3756
Versi kebijakan 3756
Dokumen kebijakan JSON 3756
Pelajari selengkapnya 3763
AWSServiceRoleForUserSubscriptions 3763
Menggunakan kebijakan ini 3763
Detail kebijakan 3763
Versi kebijakan 3763
Dokumen kebijakan JSON 3764
Pelajari selengkapnya 3765
AWSServiceRolePolicyForBackupReports 3765
Menggunakan kebijakan ini 3765
Detail kebijakan 3765
Versi kebijakan 3766
Dokumen kebijakan JSON 3766
Pelajari selengkapnya 3767
AWSServiceRolePolicyForBackupRestoreTesting 3767
Menggunakan kebijakan ini 3767
Detail kebijakan 3768
Versi kebijakan 3768
Dokumen kebijakan JSON 3768
Pelajari selengkapnya 3771
AWSServiceRolePolicyForWorkspacesInstances 3771
Menggunakan kebijakan ini 3771
Detail kebijakan 3771
Versi kebijakan 3771
Dokumen kebijakan JSON 3772
Pelajari selengkapnya 3773
AWSShieldDRTAccessPolicy 3774
Menggunakan kebijakan ini 3774
Detail kebijakan 3774
Versi kebijakan 3774
Dokumen kebijakan JSON 3774
Pelajari selengkapnya 3775

AWSShieldServiceRolePolicy 3775
Menggunakan kebijakan ini 3776
Detail kebijakan 3776
Versi kebijakan 3776
Dokumen kebijakan JSON 3776
Pelajari selengkapnya 3777
AWSSocialMessagingServiceRolePolicy 3777
Menggunakan kebijakan ini 3777
Detail kebijakan 3777
Versi kebijakan 3777
Dokumen kebijakan JSON 3777
Pelajari selengkapnya 3778
AWSSSMForSAPServiceLinkedRolePolicy 3778
Menggunakan kebijakan ini 3778
Detail kebijakan 3778
Versi kebijakan 3779
Dokumen kebijakan JSON 3779
Pelajari selengkapnya 3787
AWSSSMOpsInsightsServiceRolePolicy 3787
Menggunakan kebijakan ini 3788
Detail kebijakan 3788
Versi kebijakan 3788
Dokumen kebijakan JSON 3788
Pelajari selengkapnya 3789
AWSSSODirectoryAdministrator 3789
Menggunakan kebijakan ini 3789
Detail kebijakan 3789
Versi kebijakan 3789
Dokumen kebijakan JSON 3790
Pelajari selengkapnya 3790
AWSSSODirectoryReadOnly 3791
Menggunakan kebijakan ini 3791
Detail kebijakan 3791
Versi kebijakan 3791
Dokumen kebijakan JSON 3791
Pelajari selengkapnya 3792

AWSSSOMasterAccountAdministrator 3792
Menggunakan kebijakan ini 3793
Detail kebijakan 3793
Versi kebijakan 3793
Dokumen kebijakan JSON 3793
Pelajari selengkapnya 3796
AWSSSOMemberAccountAdministrator 3796
Menggunakan kebijakan ini 3796
Detail kebijakan 3797
Versi kebijakan 3797
Dokumen kebijakan JSON 3797
Pelajari selengkapnya 3799
AWSSSOReadOnly 3799
Menggunakan kebijakan ini 3799
Detail kebijakan 3800
Versi kebijakan 3800
Dokumen kebijakan JSON 3800
Pelajari selengkapnya 3801
AWSSSOServiceRolePolicy 3802
Menggunakan kebijakan ini 3802
Detail kebijakan 3802
Versi kebijakan 3802
Dokumen kebijakan JSON 3802
Pelajari selengkapnya 3806
AWSStepFunctionsConsoleFullAccess 3806
Menggunakan kebijakan ini 3806
Detail kebijakan 3806
Versi kebijakan 3807
Dokumen kebijakan JSON 3807
Pelajari selengkapnya 3807
AWSStepFunctionsFullAccess 3808
Menggunakan kebijakan ini 3808
Detail kebijakan 3808
Versi kebijakan 3808
Dokumen kebijakan JSON 3808
Pelajari selengkapnya 3809

AWSStepFunctionsReadOnlyAccess 3809
Menggunakan kebijakan ini 3809
Detail kebijakan 3809
Versi kebijakan 3809
Dokumen kebijakan JSON 3810
Pelajari selengkapnya 3810
AWSStorageGatewayFullAccess 3811
Menggunakan kebijakan ini 3811
Detail kebijakan 3811
Versi kebijakan 3811
Dokumen kebijakan JSON 3811
Pelajari selengkapnya 3812
AWSStorageGatewayReadOnlyAccess 3812
Menggunakan kebijakan ini 3812
Detail kebijakan 3812
Versi kebijakan 3813
Dokumen kebijakan JSON 3813
Pelajari selengkapnya 3813
AWSStorageGatewayServiceRolePolicy 3814
Menggunakan kebijakan ini 3814
Detail kebijakan 3814
Versi kebijakan 3814
Dokumen kebijakan JSON 3814
Pelajari selengkapnya 3815
AWSSupplyChainFederationAdminAccess 3815
Menggunakan kebijakan ini 3815
Detail kebijakan 3815
Versi kebijakan 3816
Dokumen kebijakan JSON 3816
Pelajari selengkapnya 3822
AWSSupportAccess 3823
Menggunakan kebijakan ini 3823
Detail kebijakan 3823
Versi kebijakan 3823
Dokumen kebijakan JSON 3823
Pelajari selengkapnya 3824

AWSSupportAppFullAccess 3824
Menggunakan kebijakan ini 3824
Detail kebijakan 3824
Versi kebijakan 3824
Dokumen kebijakan JSON 3825
Pelajari selengkapnya 3825
AWSSupportAppReadOnlyAccess 3826
Menggunakan kebijakan ini 3826
Detail kebijakan 3826
Versi kebijakan 3826
Dokumen kebijakan JSON 3826
Pelajari selengkapnya 3827
AWSSupportPlansFullAccess 3827
Menggunakan kebijakan ini 3827
Detail kebijakan 3827
Versi kebijakan 3827
Dokumen kebijakan JSON 3828
Pelajari selengkapnya 3829
AWSSupportPlansReadOnlyAccess 3829
Menggunakan kebijakan ini 3829
Detail kebijakan 3829
Versi kebijakan 3829
Dokumen kebijakan JSON 3829
Pelajari selengkapnya 3830
AWSSupportPlansServiceRolePolicy 3830
Menggunakan kebijakan ini 3830
Detail kebijakan 3830
Versi kebijakan 3831
Dokumen kebijakan JSON 3831
Pelajari selengkapnya 3831
AWSSupportServiceRolePolicy 3832
Menggunakan kebijakan ini 3832
Detail kebijakan 3832
Versi kebijakan 3832
Dokumen kebijakan JSON 3832
Pelajari selengkapnya 3938

AWSSystemsManagerAccountDiscoveryServicePolicy 3938
Menggunakan kebijakan ini 3938
Detail kebijakan 3938
Versi kebijakan 3938
Dokumen kebijakan JSON 3939
Pelajari selengkapnya 3939
AWSSystemsManagerChangeManagementServicePolicy 3939
Menggunakan kebijakan ini 3939
Detail kebijakan 3940
Versi kebijakan 3940
Dokumen kebijakan JSON 3940
Pelajari selengkapnya 3942
AWSSystemsManagerEnableConfigRecordingExecutionPolicy 3943
Menggunakan kebijakan ini 3943
Detail kebijakan 3943
Versi kebijakan 3943
Dokumen kebijakan JSON 3943
Pelajari selengkapnya 3945
AWSSystemsManagerEnableExplorerExecutionPolicy 3946
Menggunakan kebijakan ini 3946
Detail kebijakan 3946
Versi kebijakan 3946
Dokumen kebijakan JSON 3946
Pelajari selengkapnya 3948
AWSSystemsManagerForSAPFullAccess 3948
Menggunakan kebijakan ini 3948
Detail kebijakan 3948
Versi kebijakan 3948
Dokumen kebijakan JSON 3948
Pelajari selengkapnya 3950
AWSSystemsManagerForSAPReadOnlyAccess 3950
Menggunakan kebijakan ini 3950
Detail kebijakan 3950
Versi kebijakan 3950
Dokumen kebijakan JSON 3950
Pelajari selengkapnya 3951

AWSSystemsManagerJustInTimeAccessServicePolicy 3951
Menggunakan kebijakan ini 3951
Detail kebijakan 3951
Versi kebijakan 3952
Dokumen kebijakan JSON 3952
Pelajari selengkapnya 3957
AWSSystemsManagerJustInTimeAccessTokenPolicy 3957
Menggunakan kebijakan ini 3957
Detail kebijakan 3957
Versi kebijakan 3958
Dokumen kebijakan JSON 3958
Pelajari selengkapnya 3961
AWSSystemsManagerJustInTimeAccessTokenSessionPolicy 3961
Menggunakan kebijakan ini 3961
Detail kebijakan 3961
Versi kebijakan 3961
Dokumen kebijakan JSON 3962
Pelajari selengkapnya 3964
AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy 3964
Menggunakan kebijakan ini 3965
Detail kebijakan 3965
Versi kebijakan 3965
Dokumen kebijakan JSON 3965
Pelajari selengkapnya 3969
AWSSystemsManagerNotificationsServicePolicy 3969
Menggunakan kebijakan ini 3970
Detail kebijakan 3970
Versi kebijakan 3970
Dokumen kebijakan JSON 3970
Pelajari selengkapnya 3971
AWSSystemsManagerOpsDataSyncServiceRolePolicy 3972
Menggunakan kebijakan ini 3972
Detail kebijakan 3972
Versi kebijakan 3972
Dokumen kebijakan JSON 3972
Pelajari selengkapnya 3976

AWSThinkboxAssetServerPolicy 3976
Menggunakan kebijakan ini 3976
Detail kebijakan 3976
Versi kebijakan 3976
Dokumen kebijakan JSON 3977
Pelajari selengkapnya 3977
AWSThinkboxAWSPortalAdminPolicy 3978
Menggunakan kebijakan ini 3978
Detail kebijakan 3978
Versi kebijakan 3978
Dokumen kebijakan JSON 3978
Pelajari selengkapnya 3988
AWSThinkboxAWSPortalGatewayPolicy 3988
Menggunakan kebijakan ini 3989
Detail kebijakan 3989
Versi kebijakan 3989
Dokumen kebijakan JSON 3989
Pelajari selengkapnya 3991
AWSThinkboxAWSPortalWorkerPolicy 3991
Menggunakan kebijakan ini 3991
Detail kebijakan 3991
Versi kebijakan 3992
Dokumen kebijakan JSON 3992
Pelajari selengkapnya 3994
AWSThinkboxDeadlineResourceTrackerAccessPolicy 3994
Menggunakan kebijakan ini 3994
Detail kebijakan 3994
Versi kebijakan 3994
Dokumen kebijakan JSON 3995
Pelajari selengkapnya 3997
AWSThinkboxDeadlineResourceTrackerAdminPolicy 3998
Menggunakan kebijakan ini 3998
Detail kebijakan 3998
Versi kebijakan 3998
Dokumen kebijakan JSON 3998
Pelajari selengkapnya 4004

AWSThinkboxDeadlineSpotEventPluginAdminPolicy 4004
Menggunakan kebijakan ini 4005
Detail kebijakan 4005
Versi kebijakan 4005
Dokumen kebijakan JSON 4005
Pelajari selengkapnya 4008
AWSThinkboxDeadlineSpotEventPluginWorkerPolicy 4008
Menggunakan kebijakan ini 4008
Detail kebijakan 4008
Versi kebijakan 4009
Dokumen kebijakan JSON 4009
Pelajari selengkapnya 4010
AWSTransferConsoleFullAccess 4010
Menggunakan kebijakan ini 4010
Detail kebijakan 4011
Versi kebijakan 4011
Dokumen kebijakan JSON 4011
Pelajari selengkapnya 4012
AWSTransferFullAccess 4012
Menggunakan kebijakan ini 4012
Detail kebijakan 4012
Versi kebijakan 4013
Dokumen kebijakan JSON 4013
Pelajari selengkapnya 4014
AWSTransferLoggingAccess 4014
Menggunakan kebijakan ini 4014
Detail kebijakan 4014
Versi kebijakan 4014
Dokumen kebijakan JSON 4014
Pelajari selengkapnya 4015
AWSTransferReadOnlyAccess 4015
Menggunakan kebijakan ini 4015
Detail kebijakan 4015
Versi kebijakan 4016
Dokumen kebijakan JSON 4016
Pelajari selengkapnya 4016

AWSTransferServiceRolePolicy 4016
Menggunakan kebijakan ini 4017
Detail kebijakan 4017
Versi kebijakan 4017
Dokumen kebijakan JSON 4017
Pelajari selengkapnya 4019
AWSTransformApplicationDeploymentPolicy 4019
Menggunakan kebijakan ini 4019
Detail kebijakan 4019
Versi kebijakan 4019
Dokumen kebijakan JSON 4020
Pelajari selengkapnya 4028
AWSTransformApplicationECSDeploymentPolicy 4028
Menggunakan kebijakan ini 4028
Detail kebijakan 4028
Versi kebijakan 4029
Dokumen kebijakan JSON 4029
Pelajari selengkapnya 4037
AWSTransformCustomExecuteTransformations 4037
Menggunakan kebijakan ini 4037
Detail kebijakan 4037
Versi kebijakan 4038
Dokumen kebijakan JSON 4038
Pelajari selengkapnya 4039
AWSTransformCustomFullAccess 4039
Menggunakan kebijakan ini 4039
Detail kebijakan 4039
Versi kebijakan 4039
Dokumen kebijakan JSON 4040
Pelajari selengkapnya 4040
AWSTransformCustomManageTransformations 4041
Menggunakan kebijakan ini 4041
Detail kebijakan 4041
Versi kebijakan 4041
Dokumen kebijakan JSON 4041
Pelajari selengkapnya 4042

AWSTransformInfrastructureExecutorAccessBatch 4043
Menggunakan kebijakan ini 4043
Detail kebijakan 4043
Versi kebijakan 4043
Dokumen kebijakan JSON 4043
Pelajari selengkapnya 4050
AWSTransformInfrastructureExecutorAccessEC2 4050
Menggunakan kebijakan ini 4051
Detail kebijakan 4051
Versi kebijakan 4051
Dokumen kebijakan JSON 4051
Pelajari selengkapnya 4058
AWSTransformLandingZoneAgentPolicy 4059
Menggunakan kebijakan ini 4059
Detail kebijakan 4059
Versi kebijakan 4059
Dokumen kebijakan JSON 4059
Pelajari selengkapnya 4067
AWSTransformNetworkMigrationAgentPolicy 4067
Menggunakan kebijakan ini 4067
Detail kebijakan 4067
Versi kebijakan 4068
Dokumen kebijakan JSON 4068
Pelajari selengkapnya 4096
AWSTransformRevenueAttributionPolicy 4096
Menggunakan kebijakan ini 4096
Detail kebijakan 4096
Versi kebijakan 4097
Dokumen kebijakan JSON 4097
Pelajari selengkapnya 4097
AWSTransformSecretsManagerConnectorPolicy 4098
Menggunakan kebijakan ini 4098
Detail kebijakan 4098
Versi kebijakan 4098
Dokumen kebijakan JSON 4098
Pelajari selengkapnya 4100

AWSTransformSecurityAgentExecutorAccess 4100
Menggunakan kebijakan ini 4100
Detail kebijakan 4100
Versi kebijakan 4100
Dokumen kebijakan JSON 4101
Pelajari selengkapnya 4103
AWSTransformServerMigrationAgentPolicy 4103
Menggunakan kebijakan ini 4103
Detail kebijakan 4103
Versi kebijakan 4103
Dokumen kebijakan JSON 4104
Pelajari selengkapnya 4127
AWSTrustedAdvisorPriorityFullAccess 4128
Menggunakan kebijakan ini 4128
Detail kebijakan 4128
Versi kebijakan 4128
Dokumen kebijakan JSON 4128
Pelajari selengkapnya 4130
AWSTrustedAdvisorPriorityReadOnlyAccess 4130
Menggunakan kebijakan ini 4130
Detail kebijakan 4131
Versi kebijakan 4131
Dokumen kebijakan JSON 4131
Pelajari selengkapnya 4132
AWSTrustedAdvisorReportingServiceRolePolicy 4132
Menggunakan kebijakan ini 4132
Detail kebijakan 4132
Versi kebijakan 4133
Dokumen kebijakan JSON 4133
Pelajari selengkapnya 4133
AWSTrustedAdvisorServiceRolePolicy 4134
Menggunakan kebijakan ini 4134
Detail kebijakan 4134
Versi kebijakan 4134
Dokumen kebijakan JSON 4134
Pelajari selengkapnya 4137

AWSUserAttributeCostAllocationPolicy 4137
Menggunakan kebijakan ini 4138
Detail kebijakan 4138
Versi kebijakan 4138
Dokumen kebijakan JSON 4138
Pelajari selengkapnya 4138
AWSUserNotificationsServiceLinkedRolePolicy 4139
Menggunakan kebijakan ini 4139
Detail kebijakan 4139
Versi kebijakan 4139
Dokumen kebijakan JSON 4139
Pelajari selengkapnya 4141
AWSVendorInsightsAssessorFullAccess 4141
Menggunakan kebijakan ini 4141
Detail kebijakan 4141
Versi kebijakan 4142
Dokumen kebijakan JSON 4142
Pelajari selengkapnya 4143
AWSVendorInsightsAssessorReadOnly 4143
Menggunakan kebijakan ini 4143
Detail kebijakan 4143
Versi kebijakan 4144
Dokumen kebijakan JSON 4144
Pelajari selengkapnya 4144
AWSVendorInsightsVendorFullAccess 4145
Menggunakan kebijakan ini 4145
Detail kebijakan 4145
Versi kebijakan 4145
Dokumen kebijakan JSON 4145
Pelajari selengkapnya 4147
AWSVendorInsightsVendorReadOnly 4147
Menggunakan kebijakan ini 4147
Detail kebijakan 4147
Versi kebijakan 4148
Dokumen kebijakan JSON 4148
Pelajari selengkapnya 4149

AWSVPCFlowLogsServiceRolePolicy 4149
Menggunakan kebijakan ini 4149
Detail kebijakan 4149
Versi kebijakan 4149
Dokumen kebijakan JSON 4150
Pelajari selengkapnya 4151
AWSVpcLatticeServiceRolePolicy 4151
Menggunakan kebijakan ini 4151
Detail kebijakan 4152
Versi kebijakan 4152
Dokumen kebijakan JSON 4152
Pelajari selengkapnya 4155
AWSVPCS2SVpnServiceRolePolicy 4155
Menggunakan kebijakan ini 4155
Detail kebijakan 4155
Versi kebijakan 4155
Dokumen kebijakan JSON 4155
Pelajari selengkapnya 4157
AWSVPCTransitGatewayServiceRolePolicy 4157
Menggunakan kebijakan ini 4157
Detail kebijakan 4157
Versi kebijakan 4157
Dokumen kebijakan JSON 4157
Pelajari selengkapnya 4158
AWSVPCVerifiedAccessServiceRolePolicy 4158
Menggunakan kebijakan ini 4158
Detail kebijakan 4158
Versi kebijakan 4159
Dokumen kebijakan JSON 4159
Pelajari selengkapnya 4160
AWSWAFConsoleFullAccess 4161
Menggunakan kebijakan ini 4161
Detail kebijakan 4161
Versi kebijakan 4161
Dokumen kebijakan JSON 4161
Pelajari selengkapnya 4170

AWSWAFConsoleReadOnlyAccess 4171
Menggunakan kebijakan ini 4171
Detail kebijakan 4171
Versi kebijakan 4171
Dokumen kebijakan JSON 4171
Pelajari selengkapnya 4179
AWSWAFFullAccess 4179
Menggunakan kebijakan ini 4179
Detail kebijakan 4179
Versi kebijakan 4180
Dokumen kebijakan JSON 4180
Pelajari selengkapnya 4186
AWSWAFReadOnlyAccess 4186
Menggunakan kebijakan ini 4186
Detail kebijakan 4186
Versi kebijakan 4186
Dokumen kebijakan JSON 4186
Pelajari selengkapnya 4191
AWSWellArchitectedAgentOrganizationsServiceRolePolicy 4191
Menggunakan kebijakan ini 4191
Detail kebijakan 4191
Versi kebijakan 4191
Dokumen kebijakan JSON 4192
Pelajari selengkapnya 4192
AWSWellArchitectedAgentResourceScanningServiceRolePolicy 4192
Menggunakan kebijakan ini 4193
Detail kebijakan 4193
Versi kebijakan 4193
Dokumen kebijakan JSON 4193
Pelajari selengkapnya 4257
AWSWellArchitectedDiscoveryServiceRolePolicy 4258
Menggunakan kebijakan ini 4258
Detail kebijakan 4258
Versi kebijakan 4258
Dokumen kebijakan JSON 4258
Pelajari selengkapnya 4260

AWSWellArchitectedOrganizationsServiceRolePolicy 4260
Menggunakan kebijakan ini 4260
Detail kebijakan 4260
Versi kebijakan 4260
Dokumen kebijakan JSON 4261
Pelajari selengkapnya 4261
AWSWickrFullAccess 4261
Menggunakan kebijakan ini 4261
Detail kebijakan 4262
Versi kebijakan 4262
Dokumen kebijakan JSON 4262
Pelajari selengkapnya 4262
AWSXrayCrossAccountSharingConfiguration 4263
Menggunakan kebijakan ini 4263
Detail kebijakan 4263
Versi kebijakan 4263
Dokumen kebijakan JSON 4263
Pelajari selengkapnya 4264
AWSXRayDaemonWriteAccess 4264
Menggunakan kebijakan ini 4264
Detail kebijakan 4265
Versi kebijakan 4265
Dokumen kebijakan JSON 4265
Pelajari selengkapnya 4265
AWSXrayFullAccess 4266
Menggunakan kebijakan ini 4266
Detail kebijakan 4266
Versi kebijakan 4266
Dokumen kebijakan JSON 4266
Pelajari selengkapnya 4267
AWSXrayReadOnlyAccess 4267
Menggunakan kebijakan ini 4267
Detail kebijakan 4267
Versi kebijakan 4267
Dokumen kebijakan JSON 4268
Pelajari selengkapnya 4268

AWSXrayWriteOnlyAccess 4269
Menggunakan kebijakan ini 4269
Detail kebijakan 4269
Versi kebijakan 4269
Dokumen kebijakan JSON 4269
Pelajari selengkapnya 4270
AWSZonalAutoshiftPracticeRunSLRPolicy 4270
Menggunakan kebijakan ini 4270
Detail kebijakan 4270
Versi kebijakan 4271
Dokumen kebijakan JSON 4271
Pelajari selengkapnya 4272
AWSZoneGroupAccessManagementServiceRolePolicy 4272
Menggunakan kebijakan ini 4272
Detail kebijakan 4272
Versi kebijakan 4272
Dokumen kebijakan JSON 4273
Pelajari selengkapnya 4273
BatchServiceRolePolicy 4273
Menggunakan kebijakan ini 4273
Detail kebijakan 4274
Versi kebijakan 4274
Dokumen kebijakan JSON 4274
Pelajari selengkapnya 4281
BedrockAgentCoreFullAccess 4281
Menggunakan kebijakan ini 4281
Detail kebijakan 4281
Versi kebijakan 4281
Dokumen kebijakan JSON 4281
Pelajari selengkapnya 4293
BedrockAgentCoreNetworkServiceRolePolicy 4293
Menggunakan kebijakan ini 4293
Detail kebijakan 4293
Versi kebijakan 4293
Dokumen kebijakan JSON 4294
Pelajari selengkapnya 4296

BedrockAgentCoreRuntimeIdentityServiceRolePolicy 4296
Menggunakan kebijakan ini 4296
Detail kebijakan 4296
Versi kebijakan 4296
Dokumen kebijakan JSON 4296
Pelajari selengkapnya 4297
BedrockAgentCoreRuntimeInstancesInstanceRolePolicy 4297
Menggunakan kebijakan ini 4297
Detail kebijakan 4297
Versi kebijakan 4298
Dokumen kebijakan JSON 4298
Pelajari selengkapnya 4298
BedrockAgentCoreRuntimeInstancesOperatorRolePolicy 4298
Menggunakan kebijakan ini 4299
Detail kebijakan 4299
Versi kebijakan 4299
Dokumen kebijakan JSON 4299
Pelajari selengkapnya 4306
Billing 4306
Menggunakan kebijakan ini 4307
Detail kebijakan 4307
Versi kebijakan 4307
Dokumen kebijakan JSON 4307
Pelajari selengkapnya 4311
BudgetsServiceRolePolicy 4311
Menggunakan kebijakan ini 4311
Detail kebijakan 4311
Versi kebijakan 4312
Dokumen kebijakan JSON 4312
Pelajari selengkapnya 4312
CertificateManagerServiceRolePolicy 4312
Menggunakan kebijakan ini 4313
Detail kebijakan 4313
Versi kebijakan 4313
Dokumen kebijakan JSON 4313
Pelajari selengkapnya 4314

ClientVPNServiceConnectionsRolePolicy 4314
Menggunakan kebijakan ini 4314
Detail kebijakan 4314
Versi kebijakan 4314
Dokumen kebijakan JSON 4314
Pelajari selengkapnya 4315
ClientVPNServiceRolePolicy 4315
Menggunakan kebijakan ini 4315
Detail kebijakan 4315
Versi kebijakan 4315
Dokumen kebijakan JSON 4316
Pelajari selengkapnya 4316
CloudFormationStackSetsOrgAdminServiceRolePolicy 4317
Menggunakan kebijakan ini 4317
Detail kebijakan 4317
Versi kebijakan 4317
Dokumen kebijakan JSON 4317
Pelajari selengkapnya 4318
CloudFormationStackSetsOrgMemberServiceRolePolicy 4318
Menggunakan kebijakan ini 4318
Detail kebijakan 4318
Versi kebijakan 4319
Dokumen kebijakan JSON 4319
Pelajari selengkapnya 4320
CloudFrontFullAccess 4320
Menggunakan kebijakan ini 4320
Detail kebijakan 4321
Versi kebijakan 4321
Dokumen kebijakan JSON 4321
Pelajari selengkapnya 4323
CloudFrontReadOnlyAccess 4323
Menggunakan kebijakan ini 4323
Detail kebijakan 4323
Versi kebijakan 4324
Dokumen kebijakan JSON 4324
Pelajari selengkapnya 4325

CloudHSMServiceRolePolicy 4325
Menggunakan kebijakan ini 4325
Detail kebijakan 4325
Versi kebijakan 4325
Dokumen kebijakan JSON 4326
Pelajari selengkapnya 4326
CloudSearchFullAccess 4326
Menggunakan kebijakan ini 4326
Detail kebijakan 4326
Versi kebijakan 4327
Dokumen kebijakan JSON 4327
Pelajari selengkapnya 4327
CloudSearchReadOnlyAccess 4327
Menggunakan kebijakan ini 4328
Detail kebijakan 4328
Versi kebijakan 4328
Dokumen kebijakan JSON 4328
Pelajari selengkapnya 4328
CloudTrailEventContext 4329
Menggunakan kebijakan ini 4329
Detail kebijakan 4329
Versi kebijakan 4329
Dokumen kebijakan JSON 4329
Pelajari selengkapnya 4331
CloudTrailServiceRolePolicy 4331
Menggunakan kebijakan ini 4331
Detail kebijakan 4331
Versi kebijakan 4332
Dokumen kebijakan JSON 4332
Pelajari selengkapnya 4333
CloudWatch-CrossAccountAccess 4334
Menggunakan kebijakan ini 4334
Detail kebijakan 4334
Versi kebijakan 4334
Dokumen kebijakan JSON 4334
Pelajari selengkapnya 4335

CloudWatchActionsEC2Access 4335
Menggunakan kebijakan ini 4335
Detail kebijakan 4335
Versi kebijakan 4335
Dokumen kebijakan JSON 4336
Pelajari selengkapnya 4336
CloudWatchAgentAdminPolicy 4336
Menggunakan kebijakan ini 4336
Detail kebijakan 4336
Versi kebijakan 4337
Dokumen kebijakan JSON 4337
Pelajari selengkapnya 4338
CloudWatchAgentServerPolicy 4338
Menggunakan kebijakan ini 4338
Detail kebijakan 4338
Versi kebijakan 4338
Dokumen kebijakan JSON 4339
Pelajari selengkapnya 4340
CloudWatchAPIKeyAccess 4340
Menggunakan kebijakan ini 4340
Detail kebijakan 4340
Versi kebijakan 4340
Dokumen kebijakan JSON 4340
Pelajari selengkapnya 4341
CloudWatchApplicationInsightsFullAccess 4341
Menggunakan kebijakan ini 4342
Detail kebijakan 4342
Versi kebijakan 4342
Dokumen kebijakan JSON 4342
Pelajari selengkapnya 4343
CloudWatchApplicationInsightsReadOnlyAccess 4344
Menggunakan kebijakan ini 4344
Detail kebijakan 4344
Versi kebijakan 4344
Dokumen kebijakan JSON 4344
Pelajari selengkapnya 4345

CloudwatchApplicationInsightsServiceLinkedRolePolicy 4345
Menggunakan kebijakan ini 4345
Detail kebijakan 4345
Versi kebijakan 4345
Dokumen kebijakan JSON 4346
Pelajari selengkapnya 4356
CloudWatchApplicationSignalsFullAccess 4356
Menggunakan kebijakan ini 4356
Detail kebijakan 4357
Versi kebijakan 4357
Dokumen kebijakan JSON 4357
Pelajari selengkapnya 4362
CloudWatchApplicationSignalsReadOnlyAccess 4362
Menggunakan kebijakan ini 4363
Detail kebijakan 4363
Versi kebijakan 4363
Dokumen kebijakan JSON 4363
Pelajari selengkapnya 4367
CloudWatchApplicationSignalsServiceRolePolicy 4367
Menggunakan kebijakan ini 4368
Detail kebijakan 4368
Versi kebijakan 4368
Dokumen kebijakan JSON 4368
Pelajari selengkapnya 4371
CloudWatchAutomaticDashboardsAccess 4371
Menggunakan kebijakan ini 4371
Detail kebijakan 4372
Versi kebijakan 4372
Dokumen kebijakan JSON 4372
Pelajari selengkapnya 4373
CloudWatchCrossAccountSharingConfiguration 4374
Menggunakan kebijakan ini 4374
Detail kebijakan 4374
Versi kebijakan 4374
Dokumen kebijakan JSON 4374
Pelajari selengkapnya 4375

CloudWatchEventsBuiltInTargetExecutionAccess 4375
Menggunakan kebijakan ini 4376
Detail kebijakan 4376
Versi kebijakan 4376
Dokumen kebijakan JSON 4376
Pelajari selengkapnya 4377
CloudWatchEventsFullAccess 4377
Menggunakan kebijakan ini 4377
Detail kebijakan 4377
Versi kebijakan 4377
Dokumen kebijakan JSON 4377
Pelajari selengkapnya 4379
CloudWatchEventsInvocationAccess 4380
Menggunakan kebijakan ini 4380
Detail kebijakan 4380
Versi kebijakan 4380
Dokumen kebijakan JSON 4380
Pelajari selengkapnya 4381
CloudWatchEventsReadOnlyAccess 4381
Menggunakan kebijakan ini 4381
Detail kebijakan 4381
Versi kebijakan 4381
Dokumen kebijakan JSON 4382
Pelajari selengkapnya 4383
CloudWatchEventsServiceRolePolicy 4383
Menggunakan kebijakan ini 4383
Detail kebijakan 4383
Versi kebijakan 4384
Dokumen kebijakan JSON 4384
Pelajari selengkapnya 4384
CloudWatchFullAccess 4385
Menggunakan kebijakan ini 4385
Detail kebijakan 4385
Versi kebijakan 4385
Dokumen kebijakan JSON 4385
Pelajari selengkapnya 4386

CloudWatchFullAccessV2 4386
Menggunakan kebijakan ini 4386
Detail kebijakan 4387
Versi kebijakan 4387
Dokumen kebijakan JSON 4387
Pelajari selengkapnya 4393
CloudWatchInternetMonitorFullAccess 4393
Menggunakan kebijakan ini 4393
Detail kebijakan 4394
Versi kebijakan 4394
Dokumen kebijakan JSON 4394
Pelajari selengkapnya 4396
CloudWatchInternetMonitorReadOnlyAccess 4396
Menggunakan kebijakan ini 4396
Detail kebijakan 4396
Versi kebijakan 4397
Dokumen kebijakan JSON 4397
Pelajari selengkapnya 4397
CloudWatchInternetMonitorServiceRolePolicy 4398
Menggunakan kebijakan ini 4398
Detail kebijakan 4398
Versi kebijakan 4398
Dokumen kebijakan JSON 4398
Pelajari selengkapnya 4399
CloudWatchLambdaApplicationSignalsExecutionRolePolicy 4400
Menggunakan kebijakan ini 4400
Detail kebijakan 4400
Versi kebijakan 4400
Dokumen kebijakan JSON 4400
Pelajari selengkapnya 4401
CloudWatchLambdaInsightsExecutionRolePolicy 4401
Menggunakan kebijakan ini 4402
Detail kebijakan 4402
Versi kebijakan 4402
Dokumen kebijakan JSON 4402
Pelajari selengkapnya 4403

CloudWatchLogsAPIKeyAccess 4403
Menggunakan kebijakan ini 4403
Detail kebijakan 4403
Versi kebijakan 4403
Dokumen kebijakan JSON 4403
Pelajari selengkapnya 4405
CloudWatchLogsCrossAccountSharingConfiguration 4405
Menggunakan kebijakan ini 4405
Detail kebijakan 4405
Versi kebijakan 4405
Dokumen kebijakan JSON 4406
Pelajari selengkapnya 4406
CloudWatchLogsFullAccess 4407
Menggunakan kebijakan ini 4407
Detail kebijakan 4407
Versi kebijakan 4407
Dokumen kebijakan JSON 4407
Pelajari selengkapnya 4408
CloudWatchLogsReadOnlyAccess 4408
Menggunakan kebijakan ini 4408
Detail kebijakan 4408
Versi kebijakan 4408
Dokumen kebijakan JSON 4409
Pelajari selengkapnya 4409
CloudWatchNetworkFlowMonitorAgentPublishPolicy 4410
Menggunakan kebijakan ini 4410
Detail kebijakan 4410
Versi kebijakan 4410
Dokumen kebijakan JSON 4410
Pelajari selengkapnya 4411
CloudWatchNetworkFlowMonitorServiceRolePolicy 4411
Menggunakan kebijakan ini 4411
Detail kebijakan 4411
Versi kebijakan 4412
Dokumen kebijakan JSON 4412
Pelajari selengkapnya 4413

CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy 4413
Menggunakan kebijakan ini 4413
Detail kebijakan 4413
Versi kebijakan 4413
Dokumen kebijakan JSON 4414
Pelajari selengkapnya 4416
CloudWatchNetworkMonitorServiceRolePolicy 4416
Menggunakan kebijakan ini 4417
Detail kebijakan 4417
Versi kebijakan 4417
Dokumen kebijakan JSON 4417
Pelajari selengkapnya 4419
CloudWatchOmniAWSIntegrationPolicy 4419
Menggunakan kebijakan ini 4419
Detail kebijakan 4419
Versi kebijakan 4419
Dokumen kebijakan JSON 4419
Pelajari selengkapnya 4432
CloudWatchOmniDomainAccessPolicy 4432
Menggunakan kebijakan ini 4432
Detail kebijakan 4432
Versi kebijakan 4432
Dokumen kebijakan JSON 4433
Pelajari selengkapnya 4433
CloudWatchOmniModelInferencePolicy 4433
Menggunakan kebijakan ini 4434
Detail kebijakan 4434
Versi kebijakan 4434
Dokumen kebijakan JSON 4434
Pelajari selengkapnya 4435
CloudWatchOmniSpaceAccessPolicy 4435
Menggunakan kebijakan ini 4435
Detail kebijakan 4436
Versi kebijakan 4436
Dokumen kebijakan JSON 4436
Pelajari selengkapnya 4447

CloudWatchOpenSearchDashboardAccess 4447
Menggunakan kebijakan ini 4448
Detail kebijakan 4448
Versi kebijakan 4448
Dokumen kebijakan JSON 4448
Pelajari selengkapnya 4450
CloudWatchOpenSearchDashboardsFullAccess 4451
Menggunakan kebijakan ini 4451
Detail kebijakan 4451
Versi kebijakan 4451
Dokumen kebijakan JSON 4451
Pelajari selengkapnya 4458
CloudWatchReadOnlyAccess 4459
Menggunakan kebijakan ini 4459
Detail kebijakan 4459
Versi kebijakan 4459
Dokumen kebijakan JSON 4459
Pelajari selengkapnya 4462
CloudWatchSyntheticsFullAccess 4462
Menggunakan kebijakan ini 4462
Detail kebijakan 4463
Versi kebijakan 4463
Dokumen kebijakan JSON 4463
Pelajari selengkapnya 4468
CloudWatchSyntheticsReadOnlyAccess 4469
Menggunakan kebijakan ini 4469
Detail kebijakan 4469
Versi kebijakan 4469
Dokumen kebijakan JSON 4469
Pelajari selengkapnya 4470
ComprehendDataAccessRolePolicy 4470
Menggunakan kebijakan ini 4470
Detail kebijakan 4470
Versi kebijakan 4470
Dokumen kebijakan JSON 4471
Pelajari selengkapnya 4471

ComprehendFullAccess 4471
Menggunakan kebijakan ini 4471
Detail kebijakan 4471
Versi kebijakan 4472
Dokumen kebijakan JSON 4472
Pelajari selengkapnya 4472
ComprehendMedicalFullAccess 4473
Menggunakan kebijakan ini 4473
Detail kebijakan 4473
Versi kebijakan 4473
Dokumen kebijakan JSON 4473
Pelajari selengkapnya 4474
ComprehendReadOnly 4474
Menggunakan kebijakan ini 4474
Detail kebijakan 4474
Versi kebijakan 4474
Dokumen kebijakan JSON 4474
Pelajari selengkapnya 4476
ComputeOptimizerAutomationServiceRolePolicy 4476
Menggunakan kebijakan ini 4476
Detail kebijakan 4476
Versi kebijakan 4476
Dokumen kebijakan JSON 4477
Pelajari selengkapnya 4478
ComputeOptimizerReadOnlyAccess 4478
Menggunakan kebijakan ini 4479
Detail kebijakan 4479
Versi kebijakan 4479
Dokumen kebijakan JSON 4479
Pelajari selengkapnya 4480
ComputeOptimizerServiceRolePolicy 4480
Menggunakan kebijakan ini 4481
Detail kebijakan 4481
Versi kebijakan 4481
Dokumen kebijakan JSON 4481
Pelajari selengkapnya 4484

ConfigConformsServiceRolePolicy 4484
Menggunakan kebijakan ini 4484
Detail kebijakan 4484
Versi kebijakan 4484
Dokumen kebijakan JSON 4485
Pelajari selengkapnya 4487
ConsoleFullAccessFromVercel 4488
Menggunakan kebijakan ini 4488
Detail kebijakan 4488
Versi kebijakan 4488
Dokumen kebijakan JSON 4488
Pelajari selengkapnya 4493
ConsoleViewOnlyAccessFromVercel 4493
Menggunakan kebijakan ini 4493
Detail kebijakan 4493
Versi kebijakan 4494
Dokumen kebijakan JSON 4494
Pelajari selengkapnya 4496
CostOptimizationHubAdminAccess 4497
Menggunakan kebijakan ini 4497
Detail kebijakan 4497
Versi kebijakan 4497
Dokumen kebijakan JSON 4497
Pelajari selengkapnya 4499
CostOptimizationHubReadOnlyAccess 4499
Menggunakan kebijakan ini 4499
Detail kebijakan 4499
Versi kebijakan 4499
Dokumen kebijakan JSON 4499
Pelajari selengkapnya 4500
CostOptimizationHubServiceRolePolicy 4500
Menggunakan kebijakan ini 4500
Detail kebijakan 4500
Versi kebijakan 4501
Dokumen kebijakan JSON 4501
Pelajari selengkapnya 4502

CustomerProfilesServiceLinkedRolePolicy 4502
Menggunakan kebijakan ini 4502
Detail kebijakan 4502
Versi kebijakan 4503
Dokumen kebijakan JSON 4503
Pelajari selengkapnya 4504
DatabaseAdministrator 4504
Menggunakan kebijakan ini 4504
Detail kebijakan 4504
Versi kebijakan 4505
Dokumen kebijakan JSON 4505
Pelajari selengkapnya 4507
DataScientist 4508
Menggunakan kebijakan ini 4508
Detail kebijakan 4508
Versi kebijakan 4508
Dokumen kebijakan JSON 4508
Pelajari selengkapnya 4513
DAXServiceRolePolicy 4513
Menggunakan kebijakan ini 4513
Detail kebijakan 4513
Versi kebijakan 4513
Dokumen kebijakan JSON 4514
Pelajari selengkapnya 4514
DBModDiscoveryAndAssessment 4514
Menggunakan kebijakan ini 4514
Detail kebijakan 4515
Versi kebijakan 4515
Dokumen kebijakan JSON 4515
Pelajari selengkapnya 4519
DBModProvisioningAndMigration 4519
Menggunakan kebijakan ini 4519
Detail kebijakan 4519
Versi kebijakan 4520
Dokumen kebijakan JSON 4520
Pelajari selengkapnya 4525

DBModVirtualSource 4525
Menggunakan kebijakan ini 4525
Detail kebijakan 4525
Versi kebijakan 4525
Dokumen kebijakan JSON 4525
Pelajari selengkapnya 4530
DeclarativePoliciesEC2Report 4530
Menggunakan kebijakan ini 4530
Detail kebijakan 4530
Versi kebijakan 4530
Dokumen kebijakan JSON 4531
Pelajari selengkapnya 4531
DynamoDBCloudWatchContributorInsightsServiceRolePolicy 4531
Menggunakan kebijakan ini 4532
Detail kebijakan 4532
Versi kebijakan 4532
Dokumen kebijakan JSON 4532
Pelajari selengkapnya 4533
DynamoDBGlobalTableSettingsManagementServiceRolePolicy 4533
Menggunakan kebijakan ini 4533
Detail kebijakan 4533
Versi kebijakan 4533
Dokumen kebijakan JSON 4534
Pelajari selengkapnya 4535
DynamoDBKinesisReplicationServiceRolePolicy 4535
Menggunakan kebijakan ini 4535
Detail kebijakan 4535
Versi kebijakan 4535
Dokumen kebijakan JSON 4535
Pelajari selengkapnya 4536
DynamoDBReplicationServiceRolePolicy 4536
Menggunakan kebijakan ini 4536
Detail kebijakan 4537
Versi kebijakan 4537
Dokumen kebijakan JSON 4537
Pelajari selengkapnya 4538

EC2ApplicationStatusChecksServiceRolePolicy 4538
Menggunakan kebijakan ini 4538
Detail kebijakan 4539
Versi kebijakan 4539
Dokumen kebijakan JSON 4539
Pelajari selengkapnya 4540
EC2FastLaunchFullAccess 4540
Menggunakan kebijakan ini 4540
Detail kebijakan 4540
Versi kebijakan 4541
Dokumen kebijakan JSON 4541
Pelajari selengkapnya 4548
EC2FastLaunchServiceRolePolicy 4548
Menggunakan kebijakan ini 4549
Detail kebijakan 4549
Versi kebijakan 4549
Dokumen kebijakan JSON 4549
Pelajari selengkapnya 4555
EC2FleetTimeShiftableServiceRolePolicy 4555
Menggunakan kebijakan ini 4555
Detail kebijakan 4555
Versi kebijakan 4556
Dokumen kebijakan JSON 4556
Pelajari selengkapnya 4557
Ec2ImageBuilderCrossAccountDistributionAccess 4557
Menggunakan kebijakan ini 4558
Detail kebijakan 4558
Versi kebijakan 4558
Dokumen kebijakan JSON 4558
Pelajari selengkapnya 4559
EC2ImageBuilderExecutionPolicy 4559
Menggunakan kebijakan ini 4559
Detail kebijakan 4559
Versi kebijakan 4559
Dokumen kebijakan JSON 4560
Pelajari selengkapnya 4575

EC2ImageBuilderLifecycleExecutionPolicy 4575
Menggunakan kebijakan ini 4575
Detail kebijakan 4575
Versi kebijakan 4576
Dokumen kebijakan JSON 4576
Pelajari selengkapnya 4578
EC2InstanceConnect 4578
Menggunakan kebijakan ini 4578
Detail kebijakan 4578
Versi kebijakan 4578
Dokumen kebijakan JSON 4579
Pelajari selengkapnya 4579
Ec2InstanceConnectEndpoint 4579
Menggunakan kebijakan ini 4579
Detail kebijakan 4579
Versi kebijakan 4580
Dokumen kebijakan JSON 4580
Pelajari selengkapnya 4582
EC2InstanceProfileForImageBuilder 4583
Menggunakan kebijakan ini 4583
Detail kebijakan 4583
Versi kebijakan 4583
Dokumen kebijakan JSON 4583
Pelajari selengkapnya 4586
EC2InstanceProfileForImageBuilderECRContainerBuilds 4586
Menggunakan kebijakan ini 4586
Detail kebijakan 4586
Versi kebijakan 4587
Dokumen kebijakan JSON 4587
Pelajari selengkapnya 4588
ECRReplicationServiceRolePolicy 4588
Menggunakan kebijakan ini 4589
Detail kebijakan 4589
Versi kebijakan 4589
Dokumen kebijakan JSON 4589
Pelajari selengkapnya 4590

ECRTemplateServiceRolePolicy 4590
Menggunakan kebijakan ini 4590
Detail kebijakan 4590
Versi kebijakan 4590
Dokumen kebijakan JSON 4590
Pelajari selengkapnya 4591
ElastiCacheServiceRolePolicy 4591
Menggunakan kebijakan ini 4591
Detail kebijakan 4591
Versi kebijakan 4592
Dokumen kebijakan JSON 4592
Pelajari selengkapnya 4594
ElasticLoadBalancingFullAccess 4594
Menggunakan kebijakan ini 4594
Detail kebijakan 4594
Versi kebijakan 4594
Dokumen kebijakan JSON 4595
Pelajari selengkapnya 4596
ElasticLoadBalancingReadOnly 4596
Menggunakan kebijakan ini 4596
Detail kebijakan 4596
Versi kebijakan 4597
Dokumen kebijakan JSON 4597
Pelajari selengkapnya 4598
ElementalActivationsDownloadSoftwareAccess 4598
Menggunakan kebijakan ini 4598
Detail kebijakan 4598
Versi kebijakan 4598
Dokumen kebijakan JSON 4599
Pelajari selengkapnya 4599
ElementalActivationsFullAccess 4599
Menggunakan kebijakan ini 4599
Detail kebijakan 4600
Versi kebijakan 4600
Dokumen kebijakan JSON 4600
Pelajari selengkapnya 4600

ElementalActivationsGenerateLicenses 4601
Menggunakan kebijakan ini 4601
Detail kebijakan 4601
Versi kebijakan 4601
Dokumen kebijakan JSON 4601
Pelajari selengkapnya 4602
ElementalActivationsReadOnlyAccess 4602
Menggunakan kebijakan ini 4602
Detail kebijakan 4602
Versi kebijakan 4602
Dokumen kebijakan JSON 4603
Pelajari selengkapnya 4603
ElementalAppliancesSoftwareFullAccess 4603
Menggunakan kebijakan ini 4603
Detail kebijakan 4603
Versi kebijakan 4604
Dokumen kebijakan JSON 4604
Pelajari selengkapnya 4604
ElementalAppliancesSoftwareReadOnlyAccess 4604
Menggunakan kebijakan ini 4605
Detail kebijakan 4605
Versi kebijakan 4605
Dokumen kebijakan JSON 4605
Pelajari selengkapnya 4606
ElementalSupportCenterFullAccess 4606
Menggunakan kebijakan ini 4606
Detail kebijakan 4606
Versi kebijakan 4606
Dokumen kebijakan JSON 4606
Pelajari selengkapnya 4607
EMRDescribeClusterPolicyForEMRWAL 4607
Menggunakan kebijakan ini 4607
Detail kebijakan 4607
Versi kebijakan 4608
Dokumen kebijakan JSON 4608
Pelajari selengkapnya 4608

EndUserMessagingServiceRolePolicy 4608
Menggunakan kebijakan ini 4609
Detail kebijakan 4609
Versi kebijakan 4609
Dokumen kebijakan JSON 4609
Pelajari selengkapnya 4610
FinOpsAgentAgentPolicy 4610
Menggunakan kebijakan ini 4610
Detail kebijakan 4610
Versi kebijakan 4610
Dokumen kebijakan JSON 4610
Pelajari selengkapnya 4615
FinOpsAgentOperatorPolicy 4615
Menggunakan kebijakan ini 4615
Detail kebijakan 4615
Versi kebijakan 4615
Dokumen kebijakan JSON 4615
Pelajari selengkapnya 4616
FMSServiceRolePolicy 4617
Menggunakan kebijakan ini 4617
Detail kebijakan 4617
Versi kebijakan 4617
Dokumen kebijakan JSON 4617
Pelajari selengkapnya 4634
FSxDeleteServiceLinkedRoleAccess 4634
Menggunakan kebijakan ini 4634
Detail kebijakan 4634
Versi kebijakan 4635
Dokumen kebijakan JSON 4635
Pelajari selengkapnya 4635
GameLiftContainerFleetPolicy 4635
Menggunakan kebijakan ini 4636
Detail kebijakan 4636
Versi kebijakan 4636
Dokumen kebijakan JSON 4636
Pelajari selengkapnya 4637

GameLiftGameServerGroupPolicy 4638
Menggunakan kebijakan ini 4638
Detail kebijakan 4638
Versi kebijakan 4638
Dokumen kebijakan JSON 4638
Pelajari selengkapnya 4640
GitLabDuoWithAmazonQPermissionsPolicy 4640
Menggunakan kebijakan ini 4640
Detail kebijakan 4640
Versi kebijakan 4641
Dokumen kebijakan JSON 4641
Pelajari selengkapnya 4642
GlobalAcceleratorFullAccess 4642
Menggunakan kebijakan ini 4642
Detail kebijakan 4642
Versi kebijakan 4642
Dokumen kebijakan JSON 4643
Pelajari selengkapnya 4644
GlobalAcceleratorReadOnlyAccess 4644
Menggunakan kebijakan ini 4644
Detail kebijakan 4644
Versi kebijakan 4644
Dokumen kebijakan JSON 4644
Pelajari selengkapnya 4645
GreengrassOTAUpdateArtifactAccess 4645
Menggunakan kebijakan ini 4645
Detail kebijakan 4645
Versi kebijakan 4646
Dokumen kebijakan JSON 4646
Pelajari selengkapnya 4646
GroundTruthSyntheticConsoleFullAccess 4646
Menggunakan kebijakan ini 4647
Detail kebijakan 4647
Versi kebijakan 4647
Dokumen kebijakan JSON 4647
Pelajari selengkapnya 4647

GroundTruthSyntheticConsoleReadOnlyAccess 4648
Menggunakan kebijakan ini 4648
Detail kebijakan 4648
Versi kebijakan 4648
Dokumen kebijakan JSON 4648
Pelajari selengkapnya 4649
Health_OrganizationsServiceRolePolicy 4649
Menggunakan kebijakan ini 4649
Detail kebijakan 4649
Versi kebijakan 4650
Dokumen kebijakan JSON 4650
Pelajari selengkapnya 4650
IAMAccessAdvisorReadOnly 4650
Menggunakan kebijakan ini 4651
Detail kebijakan 4651
Versi kebijakan 4651
Dokumen kebijakan JSON 4651
Pelajari selengkapnya 4652
IAMAccessAnalyzerFullAccess 4652
Menggunakan kebijakan ini 4652
Detail kebijakan 4652
Versi kebijakan 4653
Dokumen kebijakan JSON 4653
Pelajari selengkapnya 4654
IAMAccessAnalyzerReadOnlyAccess 4654
Menggunakan kebijakan ini 4654
Detail kebijakan 4654
Versi kebijakan 4654
Dokumen kebijakan JSON 4655
Pelajari selengkapnya 4655
IAMFullAccess 4655
Menggunakan kebijakan ini 4656
Detail kebijakan 4656
Versi kebijakan 4656
Dokumen kebijakan JSON 4656
Pelajari selengkapnya 4657

IAMReadOnlyAccess 4657
Menggunakan kebijakan ini 4657
Detail kebijakan 4657
Versi kebijakan 4657
Dokumen kebijakan JSON 4658
Pelajari selengkapnya 4658
IAMSelfManageServiceSpecificCredentials 4658
Menggunakan kebijakan ini 4658
Detail kebijakan 4659
Versi kebijakan 4659
Dokumen kebijakan JSON 4659
Pelajari selengkapnya 4659
IAMUserChangePassword 4660
Menggunakan kebijakan ini 4660
Detail kebijakan 4660
Versi kebijakan 4660
Dokumen kebijakan JSON 4660
Pelajari selengkapnya 4661
IAMUserSSHKeys 4661
Menggunakan kebijakan ini 4661
Detail kebijakan 4661
Versi kebijakan 4662
Dokumen kebijakan JSON 4662
Pelajari selengkapnya 4662
IVSFullAccess 4662
Menggunakan kebijakan ini 4663
Detail kebijakan 4663
Versi kebijakan 4663
Dokumen kebijakan JSON 4663
Pelajari selengkapnya 4664
IVSReadOnlyAccess 4664
Menggunakan kebijakan ini 4664
Detail kebijakan 4664
Versi kebijakan 4664
Dokumen kebijakan JSON 4664
Pelajari selengkapnya 4666

IVSRecordToS3 4666
Menggunakan kebijakan ini 4666
Detail kebijakan 4666
Versi kebijakan 4666
Dokumen kebijakan JSON 4666
Pelajari selengkapnya 4667
KafkaConnectServiceRolePolicy 4667
Menggunakan kebijakan ini 4667
Detail kebijakan 4667
Versi kebijakan 4668
Dokumen kebijakan JSON 4668
Pelajari selengkapnya 4669
KafkaServiceRolePolicy 4669
Menggunakan kebijakan ini 4669
Detail kebijakan 4670
Versi kebijakan 4670
Dokumen kebijakan JSON 4670
Pelajari selengkapnya 4672
KeyspacesCDCServiceRolePolicy 4672
Menggunakan kebijakan ini 4672
Detail kebijakan 4672
Versi kebijakan 4672
Dokumen kebijakan JSON 4673
Pelajari selengkapnya 4673
KeyspacesReplicationServiceRolePolicy 4673
Menggunakan kebijakan ini 4673
Detail kebijakan 4674
Versi kebijakan 4674
Dokumen kebijakan JSON 4674
Pelajari selengkapnya 4675
LakeFormationDataAccessServiceRolePolicy 4676
Menggunakan kebijakan ini 4676
Detail kebijakan 4676
Versi kebijakan 4676
Dokumen kebijakan JSON 4676
Pelajari selengkapnya 4677

LexBotPolicy 4677
Menggunakan kebijakan ini 4677
Detail kebijakan 4677
Versi kebijakan 4677
Dokumen kebijakan JSON 4678
Pelajari selengkapnya 4678
LexChannelPolicy 4678
Menggunakan kebijakan ini 4678
Detail kebijakan 4679
Versi kebijakan 4679
Dokumen kebijakan JSON 4679
Pelajari selengkapnya 4679
LightsailExportAccess 4680
Menggunakan kebijakan ini 4680
Detail kebijakan 4680
Versi kebijakan 4680
Dokumen kebijakan JSON 4680
Pelajari selengkapnya 4681
MediaConnectGatewayInstanceRolePolicy 4681
Menggunakan kebijakan ini 4681
Detail kebijakan 4682
Versi kebijakan 4682
Dokumen kebijakan JSON 4682
Pelajari selengkapnya 4682
MediaPackageServiceRolePolicy 4683
Menggunakan kebijakan ini 4683
Detail kebijakan 4683
Versi kebijakan 4683
Dokumen kebijakan JSON 4683
Pelajari selengkapnya 4684
MemoryDBServiceRolePolicy 4684
Menggunakan kebijakan ini 4684
Detail kebijakan 4684
Versi kebijakan 4685
Dokumen kebijakan JSON 4685
Pelajari selengkapnya 4687

MigrationHubDMSAccessServiceRolePolicy 4687
Menggunakan kebijakan ini 4687
Detail kebijakan 4687
Versi kebijakan 4688
Dokumen kebijakan JSON 4688
Pelajari selengkapnya 4689
MigrationHubServiceRolePolicy 4689
Menggunakan kebijakan ini 4689
Detail kebijakan 4689
Versi kebijakan 4689
Dokumen kebijakan JSON 4690
Pelajari selengkapnya 4691
MigrationHubSMSAccessServiceRolePolicy 4691
Menggunakan kebijakan ini 4691
Detail kebijakan 4691
Versi kebijakan 4691
Dokumen kebijakan JSON 4692
Pelajari selengkapnya 4693
MonitronServiceRolePolicy 4693
Menggunakan kebijakan ini 4693
Detail kebijakan 4693
Versi kebijakan 4693
Dokumen kebijakan JSON 4693
Pelajari selengkapnya 4694
MultiPartyApprovalFullAccess 4694
Menggunakan kebijakan ini 4694
Detail kebijakan 4694
Versi kebijakan 4695
Dokumen kebijakan JSON 4695
Pelajari selengkapnya 4697
MultiPartyApprovalReadOnlyAccess 4697
Menggunakan kebijakan ini 4697
Detail kebijakan 4698
Versi kebijakan 4698
Dokumen kebijakan JSON 4698
Pelajari selengkapnya 4700

NeptuneConsoleFullAccess 4700
Menggunakan kebijakan ini 4700
Detail kebijakan 4700
Versi kebijakan 4700
Dokumen kebijakan JSON 4701
Pelajari selengkapnya 4706
NeptuneFullAccess 4706
Menggunakan kebijakan ini 4707
Detail kebijakan 4707
Versi kebijakan 4707
Dokumen kebijakan JSON 4707
Pelajari selengkapnya 4711
NeptuneGraphReadOnlyAccess 4711
Menggunakan kebijakan ini 4711
Detail kebijakan 4711
Versi kebijakan 4712
Dokumen kebijakan JSON 4712
Pelajari selengkapnya 4713
NeptuneReadOnlyAccess 4713
Menggunakan kebijakan ini 4714
Detail kebijakan 4714
Versi kebijakan 4714
Dokumen kebijakan JSON 4714
Pelajari selengkapnya 4716
NetworkAdministrator 4716
Menggunakan kebijakan ini 4717
Detail kebijakan 4717
Versi kebijakan 4717
Dokumen kebijakan JSON 4717
Pelajari selengkapnya 4724
NetworkSecurityDirectorServiceLinkedRolePolicy 4725
Menggunakan kebijakan ini 4725
Detail kebijakan 4725
Versi kebijakan 4725
Dokumen kebijakan JSON 4725
Pelajari selengkapnya 4731

NetworkSecurityManagerServiceRolePolicy 4731
Menggunakan kebijakan ini 4731
Detail kebijakan 4731
Versi kebijakan 4731
Dokumen kebijakan JSON 4732
Pelajari selengkapnya 4740
NovaActServiceRolePolicy 4740
Menggunakan kebijakan ini 4741
Detail kebijakan 4741
Versi kebijakan 4741
Dokumen kebijakan JSON 4741
Pelajari selengkapnya 4742
OAMFullAccess 4742
Menggunakan kebijakan ini 4742
Detail kebijakan 4742
Versi kebijakan 4742
Dokumen kebijakan JSON 4742
Pelajari selengkapnya 4743
OAMReadOnlyAccess 4743
Menggunakan kebijakan ini 4743
Detail kebijakan 4743
Versi kebijakan 4743
Dokumen kebijakan JSON 4744
Pelajari selengkapnya 4744
OpensearchIngestionSelfManagedVpcePolicy 4744
Menggunakan kebijakan ini 4744
Detail kebijakan 4745
Versi kebijakan 4745
Dokumen kebijakan JSON 4745
Pelajari selengkapnya 4746
PartnerCentralAccountManagementUserRoleAssociation 4746
Menggunakan kebijakan ini 4746
Detail kebijakan 4746
Versi kebijakan 4746
Dokumen kebijakan JSON 4747
Pelajari selengkapnya 4747

PartnerCentralIncentiveBenefitManagement 4748
Menggunakan kebijakan ini 4748
Detail kebijakan 4748
Versi kebijakan 4748
Dokumen kebijakan JSON 4748
Pelajari selengkapnya 4752
PowerUserAccess 4752
Menggunakan kebijakan ini 4752
Detail kebijakan 4752
Versi kebijakan 4753
Dokumen kebijakan JSON 4753
Pelajari selengkapnya 4754
PricingPlanManagerFullAccess 4754
Menggunakan kebijakan ini 4754
Detail kebijakan 4754
Versi kebijakan 4754
Dokumen kebijakan JSON 4754
Pelajari selengkapnya 4755
PricingPlanManagerReadonlyAccess 4755
Menggunakan kebijakan ini 4755
Detail kebijakan 4756
Versi kebijakan 4756
Dokumen kebijakan JSON 4756
Pelajari selengkapnya 4756
QAppsServiceRolePolicy 4757
Menggunakan kebijakan ini 4757
Detail kebijakan 4757
Versi kebijakan 4757
Dokumen kebijakan JSON 4757
Pelajari selengkapnya 4758
QBusinessQuicksightPluginPolicy 4758
Menggunakan kebijakan ini 4758
Detail kebijakan 4758
Versi kebijakan 4758
Dokumen kebijakan JSON 4759
Pelajari selengkapnya 4759

QBusinessServiceRolePolicy 4759
Menggunakan kebijakan ini 4760
Detail kebijakan 4760
Versi kebijakan 4760
Dokumen kebijakan JSON 4760
Pelajari selengkapnya 4762
QuickSightAccessForS3StorageManagementAnalyticsReadOnly 4762
Menggunakan kebijakan ini 4762
Detail kebijakan 4762
Versi kebijakan 4762
Dokumen kebijakan JSON 4763
Pelajari selengkapnya 4763
RDSCloudHsmAuthorizationRole 4763
Menggunakan kebijakan ini 4764
Detail kebijakan 4764
Versi kebijakan 4764
Dokumen kebijakan JSON 4764
Pelajari selengkapnya 4765
ReadOnlyAccess 4765
Menggunakan kebijakan ini 4765
Detail kebijakan 4765
Versi kebijakan 4765
Dokumen kebijakan JSON 4765
Pelajari selengkapnya 4835
ReInventTicketApprovalAccess 4835
Menggunakan kebijakan ini 4835
Detail kebijakan 4835
Versi kebijakan 4835
Dokumen kebijakan JSON 4836
Pelajari selengkapnya 4836
ResourceGroupsandTagEditorFullAccess 4836
Menggunakan kebijakan ini 4836
Detail kebijakan 4836
Versi kebijakan 4837
Dokumen kebijakan JSON 4837
Pelajari selengkapnya 4837

ResourceGroupsandTagEditorReadOnlyAccess 4838
Menggunakan kebijakan ini 4838
Detail kebijakan 4838
Versi kebijakan 4838
Dokumen kebijakan JSON 4838
Pelajari selengkapnya 4839
ResourceGroupsServiceRolePolicy 4839
Menggunakan kebijakan ini 4839
Detail kebijakan 4839
Versi kebijakan 4840
Dokumen kebijakan JSON 4840
Pelajari selengkapnya 4840
ResourceGroupsTaggingAPITagUntagSupportedResources 4840
Menggunakan kebijakan ini 4841
Detail kebijakan 4841
Versi kebijakan 4841
Dokumen kebijakan JSON 4841
Pelajari selengkapnya 4849
ROSAAmazonEBSCSIDriverOperatorPolicy 4850
Menggunakan kebijakan ini 4850
Detail kebijakan 4850
Versi kebijakan 4850
Dokumen kebijakan JSON 4850
Pelajari selengkapnya 4858
ROSACloudNetworkConfigOperatorPolicy 4859
Menggunakan kebijakan ini 4859
Detail kebijakan 4859
Versi kebijakan 4859
Dokumen kebijakan JSON 4859
Pelajari selengkapnya 4860
ROSAControlPlaneOperatorPolicy 4860
Menggunakan kebijakan ini 4861
Detail kebijakan 4861
Versi kebijakan 4861
Dokumen kebijakan JSON 4861
Pelajari selengkapnya 4866

ROSAImageRegistryOperatorPolicy 4866
Menggunakan kebijakan ini 4867
Detail kebijakan 4867
Versi kebijakan 4867
Dokumen kebijakan JSON 4867
Pelajari selengkapnya 4868
ROSAIngressOperatorPolicy 4869
Menggunakan kebijakan ini 4869
Detail kebijakan 4869
Versi kebijakan 4869
Dokumen kebijakan JSON 4869
Pelajari selengkapnya 4870
ROSAInstallerPolicy 4870
Menggunakan kebijakan ini 4870
Detail kebijakan 4871
Versi kebijakan 4871
Dokumen kebijakan JSON 4871
Pelajari selengkapnya 4879
ROSAKarpenterControllerPolicy 4880
Menggunakan kebijakan ini 4880
Detail kebijakan 4880
Versi kebijakan 4880
Dokumen kebijakan JSON 4880
Pelajari selengkapnya 4887
ROSAKMSProviderPolicy 4887
Menggunakan kebijakan ini 4887
Detail kebijakan 4887
Versi kebijakan 4887
Dokumen kebijakan JSON 4888
Pelajari selengkapnya 4888
ROSAKubeControllerPolicy 4888
Menggunakan kebijakan ini 4888
Detail kebijakan 4889
Versi kebijakan 4889
Dokumen kebijakan JSON 4889
Pelajari selengkapnya 4894

ROSAManageSubscription 4894
Menggunakan kebijakan ini 4894
Detail kebijakan 4894
Versi kebijakan 4894
Dokumen kebijakan JSON 4895
Pelajari selengkapnya 4895
ROSANodePoolManagementPolicy 4896
Menggunakan kebijakan ini 4896
Detail kebijakan 4896
Versi kebijakan 4896
Dokumen kebijakan JSON 4896
Pelajari selengkapnya 4903
ROSASharedVPCEndpointPolicy 4903
Menggunakan kebijakan ini 4903
Detail kebijakan 4903
Versi kebijakan 4903
Dokumen kebijakan JSON 4904
Pelajari selengkapnya 4907
ROSASharedVPCRoute53Policy 4908
Menggunakan kebijakan ini 4908
Detail kebijakan 4908
Versi kebijakan 4908
Dokumen kebijakan JSON 4908
Pelajari selengkapnya 4909
ROSASRESupportPolicy 4910
Menggunakan kebijakan ini 4910
Detail kebijakan 4910
Versi kebijakan 4910
Dokumen kebijakan JSON 4910
Pelajari selengkapnya 4915
ROSAWorkerInstancePolicy 4915
Menggunakan kebijakan ini 4915
Detail kebijakan 4916
Versi kebijakan 4916
Dokumen kebijakan JSON 4916
Pelajari selengkapnya 4917

Route53RecoveryReadinessServiceRolePolicy 4917
Menggunakan kebijakan ini 4917
Detail kebijakan 4918
Versi kebijakan 4918
Dokumen kebijakan JSON 4918
Pelajari selengkapnya 4921
Route53ResolverServiceRolePolicy 4922
Menggunakan kebijakan ini 4922
Detail kebijakan 4922
Versi kebijakan 4922
Dokumen kebijakan JSON 4922
Pelajari selengkapnya 4923
RTBFabricServiceRolePolicy 4923
Menggunakan kebijakan ini 4923
Detail kebijakan 4923
Versi kebijakan 4923
Dokumen kebijakan JSON 4924
Pelajari selengkapnya 4926
S3StorageLensServiceRolePolicy 4926
Menggunakan kebijakan ini 4926
Detail kebijakan 4926
Versi kebijakan 4926
Dokumen kebijakan JSON 4927
Pelajari selengkapnya 4927
SageMakerStudioAdminIAMConsolePolicy 4927
Menggunakan kebijakan ini 4928
Detail kebijakan 4928
Versi kebijakan 4928
Dokumen kebijakan JSON 4928
Pelajari selengkapnya 4940
SageMakerStudioAdminIAMDefaultExecutionPolicy 4940
Menggunakan kebijakan ini 4941
Detail kebijakan 4941
Versi kebijakan 4941
Dokumen kebijakan JSON 4941
Pelajari selengkapnya 4966

SageMakerStudioAdminIAMPermissiveExecutionPolicy 4967
Menggunakan kebijakan ini 4967
Detail kebijakan 4967
Versi kebijakan 4967
Dokumen kebijakan JSON 4967
Pelajari selengkapnya 4986
SageMakerStudioAdminProjectUserRolePolicy 4986
Menggunakan kebijakan ini 4986
Detail kebijakan 4987
Versi kebijakan 4987
Dokumen kebijakan JSON 4987
Pelajari selengkapnya 4989
SageMakerStudioBedrockAgentServiceRolePolicy 4990
Menggunakan kebijakan ini 4990
Detail kebijakan 4990
Versi kebijakan 4990
Dokumen kebijakan JSON 4990
Pelajari selengkapnya 4994
SageMakerStudioBedrockChatAgentUserRolePolicy 4994
Menggunakan kebijakan ini 4994
Detail kebijakan 4994
Versi kebijakan 4994
Dokumen kebijakan JSON 4995
Pelajari selengkapnya 4999
SageMakerStudioBedrockEvaluationJobServiceRolePolicy 4999
Menggunakan kebijakan ini 4999
Detail kebijakan 4999
Versi kebijakan 4999
Dokumen kebijakan JSON 5000
Pelajari selengkapnya 5003
SageMakerStudioBedrockFlowServiceRolePolicy 5003
Menggunakan kebijakan ini 5004
Detail kebijakan 5004
Versi kebijakan 5004
Dokumen kebijakan JSON 5004
Pelajari selengkapnya 5008

SageMakerStudioBedrockFunctionExecutionRolePolicy 5008
Menggunakan kebijakan ini 5008
Detail kebijakan 5008
Versi kebijakan 5009
Dokumen kebijakan JSON 5009
Pelajari selengkapnya 5010
SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy 5010
Menggunakan kebijakan ini 5010
Detail kebijakan 5010
Versi kebijakan 5011
Dokumen kebijakan JSON 5011
Pelajari selengkapnya 5012
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy 5012
Menggunakan kebijakan ini 5012
Detail kebijakan 5012
Versi kebijakan 5012
Dokumen kebijakan JSON 5013
Pelajari selengkapnya 5018
SageMakerStudioBedrockPromptUserRolePolicy 5018
Menggunakan kebijakan ini 5019
Detail kebijakan 5019
Versi kebijakan 5019
Dokumen kebijakan JSON 5019
Pelajari selengkapnya 5021
SageMakerStudioDomainExecutionRolePolicy 5022
Menggunakan kebijakan ini 5022
Detail kebijakan 5022
Versi kebijakan 5022
Dokumen kebijakan JSON 5022
Pelajari selengkapnya 5029
SageMakerStudioDomainServiceRolePolicy 5029
Menggunakan kebijakan ini 5029
Detail kebijakan 5029
Versi kebijakan 5029
Dokumen kebijakan JSON 5030
Pelajari selengkapnya 5031

SageMakerStudioEMRContainersSystemNamespaceRolePolicy 5031
Menggunakan kebijakan ini 5031
Detail kebijakan 5031
Versi kebijakan 5031
Dokumen kebijakan JSON 5032
Pelajari selengkapnya 5033
SageMakerStudioEMRInstanceRolePolicy 5033
Menggunakan kebijakan ini 5034
Detail kebijakan 5034
Versi kebijakan 5034
Dokumen kebijakan JSON 5034
Pelajari selengkapnya 5038
SageMakerStudioEMRServiceRolePolicy 5038
Menggunakan kebijakan ini 5038
Detail kebijakan 5038
Versi kebijakan 5038
Dokumen kebijakan JSON 5039
Pelajari selengkapnya 5041
SageMakerStudioFullAccess 5041
Menggunakan kebijakan ini 5041
Detail kebijakan 5041
Versi kebijakan 5041
Dokumen kebijakan JSON 5042
Pelajari selengkapnya 5052
SageMakerStudioProjectProvisioningRolePolicy 5052
Menggunakan kebijakan ini 5052
Detail kebijakan 5052
Versi kebijakan 5052
Dokumen kebijakan JSON 5053
Pelajari selengkapnya 5122
SageMakerStudioProjectRoleMachineLearningPolicy 5122
Menggunakan kebijakan ini 5122
Detail kebijakan 5122
Versi kebijakan 5123
Dokumen kebijakan JSON 5123
Pelajari selengkapnya 5153

SageMakerStudioProjectUserRolePermissionsBoundary 5153
Menggunakan kebijakan ini 5154
Detail kebijakan 5154
Versi kebijakan 5154
Dokumen kebijakan JSON 5154
Pelajari selengkapnya 5209
SageMakerStudioProjectUserRolePolicy 5210
Menggunakan kebijakan ini 5210
Detail kebijakan 5210
Versi kebijakan 5210
Dokumen kebijakan JSON 5210
Pelajari selengkapnya 5276
SageMakerStudioQueryExecutionRolePolicy 5276
Menggunakan kebijakan ini 5277
Detail kebijakan 5277
Versi kebijakan 5277
Dokumen kebijakan JSON 5277
Pelajari selengkapnya 5279
SageMakerStudioUserIAMConsolePolicy 5279
Menggunakan kebijakan ini 5279
Detail kebijakan 5279
Versi kebijakan 5280
Dokumen kebijakan JSON 5280
Pelajari selengkapnya 5281
SageMakerStudioUserIAMDefaultExecutionPolicy 5282
Menggunakan kebijakan ini 5282
Detail kebijakan 5282
Versi kebijakan 5282
Dokumen kebijakan JSON 5282
Pelajari selengkapnya 5307
SageMakerStudioUserIAMPermissiveExecutionPolicy 5307
Menggunakan kebijakan ini 5307
Detail kebijakan 5307
Versi kebijakan 5308
Dokumen kebijakan JSON 5308
Pelajari selengkapnya 5322

SecretsManagerReadWrite 5323
Menggunakan kebijakan ini 5323
Detail kebijakan 5323
Versi kebijakan 5323
Dokumen kebijakan JSON 5323
Pelajari selengkapnya 5325
SecurityAgentWebAppAPIPolicy 5325
Menggunakan kebijakan ini 5326
Detail kebijakan 5326
Versi kebijakan 5326
Dokumen kebijakan JSON 5326
Pelajari selengkapnya 5328
SecurityAgentWebAppPolicy 5328
Menggunakan kebijakan ini 5328
Detail kebijakan 5328
Versi kebijakan 5329
Dokumen kebijakan JSON 5329
Pelajari selengkapnya 5330
SecurityAudit 5331
Menggunakan kebijakan ini 5331
Detail kebijakan 5331
Versi kebijakan 5331
Dokumen kebijakan JSON 5331
Pelajari selengkapnya 5360
SecurityLakeResourceManagementServiceRolePolicy 5360
Menggunakan kebijakan ini 5360
Detail kebijakan 5360
Versi kebijakan 5361
Dokumen kebijakan JSON 5361
Pelajari selengkapnya 5366
SecurityLakeServiceLinkedRole 5367
Menggunakan kebijakan ini 5367
Detail kebijakan 5367
Versi kebijakan 5367
Dokumen kebijakan JSON 5367
Pelajari selengkapnya 5370

ServerMigration_ServiceRole 5371
Menggunakan kebijakan ini 5371
Detail kebijakan 5371
Versi kebijakan 5371
Dokumen kebijakan JSON 5371
Pelajari selengkapnya 5376
ServerMigrationConnector 5376
Menggunakan kebijakan ini 5376
Detail kebijakan 5377
Versi kebijakan 5377
Dokumen kebijakan JSON 5377
Pelajari selengkapnya 5378
ServerMigrationServiceConsoleFullAccess 5379
Menggunakan kebijakan ini 5379
Detail kebijakan 5379
Versi kebijakan 5379
Dokumen kebijakan JSON 5379
Pelajari selengkapnya 5381
ServerMigrationServiceLaunchRole 5381
Menggunakan kebijakan ini 5381
Detail kebijakan 5381
Versi kebijakan 5382
Dokumen kebijakan JSON 5382
Pelajari selengkapnya 5385
ServerMigrationServiceRoleForInstanceValidation 5385
Menggunakan kebijakan ini 5385
Detail kebijakan 5385
Versi kebijakan 5385
Dokumen kebijakan JSON 5386
Pelajari selengkapnya 5386
ServiceQuotasFullAccess 5386
Menggunakan kebijakan ini 5386
Detail kebijakan 5386
Versi kebijakan 5387
Dokumen kebijakan JSON 5387
Pelajari selengkapnya 5388

ServiceQuotasReadOnlyAccess 5389
Menggunakan kebijakan ini 5389
Detail kebijakan 5389
Versi kebijakan 5389
Dokumen kebijakan JSON 5389
Pelajari selengkapnya 5391
ServiceQuotasServiceRolePolicy 5391
Menggunakan kebijakan ini 5391
Detail kebijakan 5391
Versi kebijakan 5391
Dokumen kebijakan JSON 5392
Pelajari selengkapnya 5392
SignInLocalDevelopmentAccess 5392
Menggunakan kebijakan ini 5392
Detail kebijakan 5392
Versi kebijakan 5393
Dokumen kebijakan JSON 5393
Pelajari selengkapnya 5393
SimpleWorkflowFullAccess 5393
Menggunakan kebijakan ini 5393
Detail kebijakan 5394
Versi kebijakan 5394
Dokumen kebijakan JSON 5394
Pelajari selengkapnya 5394
SMSVoiceServiceRolePolicy 5395
Menggunakan kebijakan ini 5395
Detail kebijakan 5395
Versi kebijakan 5395
Dokumen kebijakan JSON 5395
Pelajari selengkapnya 5396
SplitCostAllocationDataServiceRolePolicy 5396
Menggunakan kebijakan ini 5396
Detail kebijakan 5396
Versi kebijakan 5396
Dokumen kebijakan JSON 5397
Pelajari selengkapnya 5397

SSMQuickSetupRolePolicy 5397
Menggunakan kebijakan ini 5398
Detail kebijakan 5398
Versi kebijakan 5398
Dokumen kebijakan JSON 5398
Pelajari selengkapnya 5401
SupportUser 5401
Menggunakan kebijakan ini 5401
Detail kebijakan 5401
Versi kebijakan 5402
Dokumen kebijakan JSON 5402
Pelajari selengkapnya 5407
SystemAdministrator 5407
Menggunakan kebijakan ini 5407
Detail kebijakan 5407
Versi kebijakan 5408
Dokumen kebijakan JSON 5408
Pelajari selengkapnya 5414
TranslateFullAccess 5414
Menggunakan kebijakan ini 5414
Detail kebijakan 5414
Versi kebijakan 5415
Dokumen kebijakan JSON 5415
Pelajari selengkapnya 5415
TranslateReadOnly 5416
Menggunakan kebijakan ini 5416
Detail kebijakan 5416
Versi kebijakan 5416
Dokumen kebijakan JSON 5416
Pelajari selengkapnya 5417
ViewOnlyAccess 5417
Menggunakan kebijakan ini 5417
Detail kebijakan 5417
Versi kebijakan 5417
Dokumen kebijakan JSON 5418
Pelajari selengkapnya 5435

VMImportExportRoleForAWSConnector 5435
Menggunakan kebijakan ini 5435
Detail kebijakan 5436
Versi kebijakan 5436
Dokumen kebijakan JSON 5436
Pelajari selengkapnya 5437
VPCLatticeFullAccess 5437
Menggunakan kebijakan ini 5437
Detail kebijakan 5437
Versi kebijakan 5437
Dokumen kebijakan JSON 5438
Pelajari selengkapnya 5440
VPCLatticeReadOnlyAccess 5440
Menggunakan kebijakan ini 5440
Detail kebijakan 5440
Versi kebijakan 5440
Dokumen kebijakan JSON 5440
Pelajari selengkapnya 5441
VPCLatticeServicesInvokeAccess 5442
Menggunakan kebijakan ini 5442
Detail kebijakan 5442
Versi kebijakan 5442
Dokumen kebijakan JSON 5442
Pelajari selengkapnya 5443
WAFLoggingServiceRolePolicy 5443
Menggunakan kebijakan ini 5443
Detail kebijakan 5443
Versi kebijakan 5443
Dokumen kebijakan JSON 5444
Pelajari selengkapnya 5444
WAFRegionalLoggingServiceRolePolicy 5444
Menggunakan kebijakan ini 5445
Detail kebijakan 5445
Versi kebijakan 5445
Dokumen kebijakan JSON 5445
Pelajari selengkapnya 5446

WAFV2LoggingServiceRolePolicy 5446
Menggunakan kebijakan ini 5446
Detail kebijakan 5446
Versi kebijakan 5447
Dokumen kebijakan JSON 5447
Pelajari selengkapnya 5448
WellArchitectedAgentResourceScanning 5448
Menggunakan kebijakan ini 5448
Detail kebijakan 5448
Versi kebijakan 5448
Dokumen kebijakan JSON 5449
Pelajari selengkapnya 5475
WellArchitectedConsoleFullAccess 5475
Menggunakan kebijakan ini 5475
Detail kebijakan 5475
Versi kebijakan 5475
Dokumen kebijakan JSON 5476
Pelajari selengkapnya 5478
WellArchitectedConsoleReadOnlyAccess 5478
Menggunakan kebijakan ini 5479
Detail kebijakan 5479
Versi kebijakan 5479
Dokumen kebijakan JSON 5479
Pelajari selengkapnya 5480
WorkLinkServiceRolePolicy 5480
Menggunakan kebijakan ini 5480
Detail kebijakan 5480
Versi kebijakan 5480
Dokumen kebijakan JSON 5481
Pelajari selengkapnya 5481
..... 5482

Apa itu kebijakan yang AWS dikelola?

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS kebijakan terkelola dirancang untuk memberikan izin untuk banyak kasus penggunaan umum. Mereka memudahkan Anda untuk memulai dengan menetapkan izin kepada pengguna, grup, dan peran daripada jika Anda harus menulis kebijakan sendiri.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan oleh semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat AWS layanan baru diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat kebijakan AWS terkelola di Panduan Pengguna IAM.

Memahami halaman referensi kebijakan

Setiap halaman referensi kebijakan mencakup informasi berikut:

- Menggunakan kebijakan ini — Apakah Anda dapat melampirkan kebijakan ke pengguna, grup, dan peran
- Rincian kebijakan
  - Jenis — Jenis kebijakan AWS terkelola
    - `AWS managed policy`— Kebijakan AWS terkelola standar
    - `Job function policy`— Kebijakan yang sejalan dengan fungsi pekerjaan industri umum
    - `Service-linked role policy`Kebijakan yang dilampirkan pada peran terkait layanan yang memungkinkan layanan untuk melakukan tindakan atas nama Anda, seperti the section called “AmazonRDSPreviewServiceRolePolicy”
    - `Service role policy`— Kebijakan yang dirancang untuk bekerja dengan peran layanan, seperti the section called “AWSControlTowerServiceRolePolicy”
  - Waktu pembuatan — Saat kebijakan pertama kali dibuat

  - Waktu yang diedit - Saat versi kebijakan ini diedit
  - ARN - Nama Sumber Daya Amazon dari kebijakan
- Versi kebijakan — Versi izin yang diberikan oleh kebijakan
- Dokumen kebijakan JSON — Kebijakan JSON
- Pelajari selengkapnya - Tautan ke dokumentasi yang terkait dengan kebijakan AWS terkelola

Kebijakan terkelola yang tidak digunakan lagi AWS

AWS memperbarui kebijakan AWS terkelola secara berkala. Dalam kebanyakan kasus, kami menambahkan izin ke kebijakan. Ini terjadi ketika kami meluncurkan layanan atau fitur baru. Untuk meningkatkan keamanan kebijakan yang AWS dikelola, terkadang kami mengurangi ruang lingkup kebijakan. Saat kami menghapus izin dari kebijakan, kami menetapkan kebijakan ke status usang dan membuat yang baru tersedia. Saat AWS menghentikan layanan atau fitur, kami juga menghentikan kebijakan terkelola untuk fitur tersebut. AWS

Jika Anda menerima pemberitahuan email bahwa kebijakan yang Anda gunakan tidak berlaku lagi, kami sarankan Anda segera mengambil tindakan. Identifikasi perubahan kebijakan dan perbarui alur kerja Anda. Jika AWS menyediakan kebijakan penggantian, rencanakan untuk melampirkannya ke semua identitas yang terpengaruh (pengguna, grup, dan peran), lalu lepaskan kebijakan yang tidak digunakan lagi dari identitas tersebut.

Kebijakan usang memiliki karakteristik sebagai berikut:

- Itu dihapus dari panduan ini.
- Izin terus berfungsi untuk semua identitas yang saat ini dilampirkan.
- Di akun tempat kebijakan dilampirkan ke identitas, muncul di daftar Kebijakan di konsol IAM dengan ikon peringatan di sebelahnya.
- Itu tidak dapat dilampirkan pada identitas baru apa pun. Jika Anda melepaskannya dari identitas saat ini, Anda tidak dapat memasangnya kembali.
- Setelah Anda melepaskannya dari semua entitas saat ini, itu tidak lagi terlihat.

AWS kebijakan terkelola

AWS kebijakan yang dikelola

- AccessAnalyzerServiceRolePolicy
- AccountAccessManagerServiceRolePolicy
- AccountManagementFromVercel
- AdministratorAccess
- AdministratorAccess-Amplify
- AdministratorAccess-AWSElasticBeanstalk
- AgentRegistryFullAccess
- AgentRegistryReadOnlyAccess
- AIDevOpsAgentAccessPolicy
- AIDevOpsAgentActionsPolicy
- AIDevOpsAgentFullAccess
- AIDevOpsAgentReadOnlyAccess
- AIDevOpsChannelAccessPolicy
- AIDevOpsConstellationAccessPolicy
- AIDevOpsOperatorAppAccessPolicy
- AIDevOpsReleaseManagementVPCPolicy
- AIOpsAssistantIncidentReportPolicy
- AIOpsAssistantPolicy
- AIOpsConsoleAdminPolicy
- AIOpsOperatorAccess
- AIOpsReadOnlyAccess
- AlexaForBusinessDeviceSetup
- AlexaForBusinessFullAccess
- AlexaForBusinessGatewayExecution
- AlexaForBusinessLifesizeDelegatedAccessPolicy
- AlexaForBusinessNetworkProfileServicePolicy

- AlexaForBusinessPolyDelegatedAccessPolicy
- AlexaForBusinessReadOnlyAccess
- AmazonAPIGatewayAdministrator
- AmazonAPIGatewayInvokeFullAccess
- AmazonAPIGatewayPushToCloudWatchLogs
- AmazonAppFlowFullAccess
- AmazonAppFlowReadOnlyAccess
- AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy
- AmazonAppStreamFullAccess
- AmazonAppStreamPCAAccess
- AmazonAppStreamReadOnlyAccess
- AmazonAppStreamServiceAccess
- AmazonAthenaFullAccess
- AmazonAthenaServiceRolePolicy
- AmazonAugmentedAIFullAccess
- AmazonAugmentedAIHumanLoopFullAccess
- AmazonAugmentedAIIntegratedAPIAccess
- AmazonAuroraDSQLConsoleFullAccess
- AmazonAuroraDSQLFullAccess
- AmazonAuroraDSQLReadOnlyAccess
- AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy
- AmazonBedrockExternalWebSearchFullAccess
- AmazonBedrockExternalWebSearchReadOnly
- AmazonBedrockFullAccess
- AmazonBedrockLimitedAccess
- AmazonBedrockMantleFullAccess
- AmazonBedrockMantleInferenceAccess
- AmazonBedrockMantleReadOnly
- AmazonBedrockMarketplaceAccess

- AmazonBedrockReadOnly
- AmazonBedrockStudioPermissionsBoundary
- AmazonBedrockWebSearchFullAccess
- AmazonBedrockWebSearchReadOnly
- AmazonBioDiscoveryFullAccess
- AmazonBioDiscoveryInAppFullAccess
- AmazonBraketFullAccess
- AmazonBraketJobsExecutionPolicy
- AmazonBraketServiceRolePolicy
- AmazonChimeFullAccess
- AmazonChimeReadOnly
- AmazonChimeSDK
- AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy
- AmazonChimeSDKMessagingServiceRolePolicy
- AmazonChimeServiceRolePolicy
- AmazonChimeTranscriptionServiceLinkedRolePolicy
- AmazonChimeUserManagement
- AmazonChimeVoiceConnectorServiceLinkedRolePolicy
- AmazonCloudDirectoryFullAccess
- AmazonCloudDirectoryReadOnlyAccess
- AmazonCloudWatchEvidentlyFullAccess
- AmazonCloudWatchEvidentlyReadOnlyAccess
- AmazonCloudWatchEvidentlyServiceRolePolicy
- AmazonCloudWatchRUMFullAccess
- AmazonCloudWatchRUMReadOnlyAccess
- AmazonCloudWatchRUMServiceRolePolicy
- AmazonCodeCatalystFullAccess
- AmazonCodeCatalystReadOnlyAccess
- AmazonCodeCatalystSupportAccess

- AmazonCodeGuruProfilerAgentAccess
- AmazonCodeGuruProfilerFullAccess
- AmazonCodeGuruProfilerReadOnlyAccess
- AmazonCodeGuruReviewerFullAccess
- AmazonCodeGuruReviewerReadOnlyAccess
- AmazonCodeGuruReviewerServiceRolePolicy
- AmazonCodeGuruSecurityFullAccess
- AmazonCodeGuruSecurityScanAccess
- AmazonCognitoDeveloperAuthenticatedIdentities
- AmazonCognitoIdpEmailServiceRolePolicy
- AmazonCognitoIdpServiceRolePolicy
- AmazonCognitoPowerUser
- AmazonCognitoReadOnly
- AmazonCognitoUnAuthedIdentitiesSessionPolicy
- AmazonCognitoUnauthenticatedIdentities
- AmazonConnect_FullAccess
- AmazonConnectCampaignsServiceLinkedRolePolicy
- AmazonConnectReadOnlyAccess
- AmazonConnectServiceLinkedRolePolicy
- AmazonConnectSynchronizationServiceRolePolicy
- AmazonConnectVoiceIDFullAccess
- AmazonDataZoneBedrockModelConsumptionPolicy
- AmazonDataZoneBedrockModelManagementPolicy
- AmazonDataZoneDomainExecutionRolePolicy
- AmazonDataZoneEnvironmentRolePermissionsBoundary
- AmazonDataZoneFullAccess
- AmazonDataZoneFullUserAccess
- AmazonDataZoneGlueManageAccessRolePolicy
- AmazonDataZonePortalFullAccessPolicy

- AmazonDataZonePreviewConsoleFullAccess
- AmazonDataZoneProjectDeploymentPermissionsBoundary
- AmazonDataZoneProjectRolePermissionsBoundary
- AmazonDataZoneRedshiftGlueProvisioningPolicy
- AmazonDataZoneRedshiftManageAccessRolePolicy
- AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary
- AmazonDataZoneSageMakerManageAccessRolePolicy
- AmazonDataZoneSageMakerProvisioningRolePolicy
- AmazonDetectiveFullAccess
- AmazonDetectiveInvestigatorAccess
- AmazonDetectiveMemberAccess
- AmazonDetectiveOrganizationsAccess
- AmazonDetectiveServiceLinkedRolePolicy
- AmazonDevOpsGuruConsoleFullAccess
- AmazonDevOpsGuruFullAccess
- AmazonDevOpsGuruOrganizationsAccess
- AmazonDevOpsGuruReadOnlyAccess
- AmazonDevOpsGuruServiceRolePolicy
- AmazonDMSCloudWatchLogsRole
- AmazonDMSRedshiftS3Role
- AmazonDMSVPCManagementRole
- AmazonDocDB-ElasticServiceRolePolicy
- AmazonDocDBConsoleFullAccess
- AmazonDocDBElasticFullAccess
- AmazonDocDBElasticReadOnlyAccess
- AmazonDocDBFullAccess
- AmazonDocDBReadOnlyAccess
- AmazonDRSVPCManajemen
- AmazonDynamoDBFullAccess

- AmazonDynamoDBFullAccess_v2
- AmazonDynamoDBFullAccesswithDataPipeline
- AmazonDynamoDBReadOnlyAccess
- AmazonEBSCSIDriverEKSClusterScopedPolicy
- AmazonEBSCSIDriverPolicy
- AmazonEBSCSIDriverPolicyV2
- AmazonEC2ContainerRegistryFullAccess
- AmazonEC2ContainerRegistryPowerUser
- AmazonEC2ContainerRegistryPullOnly
- AmazonEC2ContainerRegistryReadOnly
- AmazonEC2ContainerServiceAutoscaleRole
- AmazonEC2ContainerServiceEventsRole
- AmazonEC2ContainerServiceforEC2Role
- AmazonEC2ContainerServiceRole
- AmazonEC2FullAccess
- AmazonEC2ImageReferencesAccessPolicy
- AmazonEC2ReadOnlyAccess
- AmazonEC2RoleforAWSCodeDeploy
- AmazonEC2RoleforAWSCodeDeployLimited
- AmazonEC2RoleforDataPipelineRole
- AmazonEC2RoleForSSM
- AmazonEC2RolePolicyForLaunchWizard
- AmazonEC2SpotFleetAutoscaleRole
- AmazonEC2SpotFleetTaggingRole
- AmazonECS_ FullAccess
- AmazonECSComputeServiceRolePolicy
- AmazonECSInfrastructureRoleforExpressGatewayServices
- AmazonECSInfrastructureRoleForGatewayHostSharedALB
- AmazonECSInfrastructureRolePolicyForLoadBalancers

- AmazonECSInfrastructureRolePolicyForManagedInstances
- AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity
- AmazonECSInfrastructureRolePolicyForVolumes
- AmazonECSInfrastructureRolePolicyForVpcLattice
- AmazonECSInstanceRolePolicyForManagedInstances
- AmazonECSServiceRolePolicy
- AmazonECSTaskExecutionRolePolicy
- AmazonEFSCSIDriverPolicy
- AmazonEKS_CNI_Policy
- AmazonEKSBlockStoragePolicy
- AmazonEKSBlockStoragePolicyV2
- AmazonEKSClusterPolicy
- AmazonEKSComputePolicy
- AmazonEKSConnectorServiceRolePolicy
- AmazonEKSDashboardConsoleReadOnly
- AmazonEKSDashboardServiceRolePolicy
- AmazonEKSFargatePodExecutionRolePolicy
- AmazonEKSForFargateServiceRolePolicy
- AmazonEKSLoadBalancingPolicy
- AmazonEKSLocalOutpostClusterPolicy
- AmazonEKSLocalOutpostServiceRolePolicy
- AmazonEKSMCPReadOnlyAccess
- AmazonEKSNetworkingPolicy
- AmazonEKSServicePolicy
- AmazonEKSServiceRolePolicy
- AmazonEKSVPCResourceController
- AmazonEKSWorkerNodeMinimalPolicy
- AmazonEKSWorkerNodePolicy
- AmazonElastiCacheFullAccess

- AmazonElastiCacheReadOnlyAccess
- AmazonElasticContainerRegistryPublicFullAccess
- AmazonElasticContainerRegistryPublicPowerUser
- AmazonElasticContainerRegistryPublicReadOnly
- AmazonElasticFileSystemClientFullAccess
- AmazonElasticFileSystemClientReadOnlyAccess
- AmazonElasticFileSystemClientReadWriteAccess
- AmazonElasticFileSystemFullAccess
- AmazonElasticFileSystemReadOnlyAccess
- AmazonElasticFileSystemServiceRolePolicy
- AmazonElasticFileSystemsUtils
- AmazonElasticMapReduceEditorsRole
- AmazonElasticMapReduceforAutoScalingRole
- AmazonElasticMapReduceforEC2Role
- AmazonElasticMapReduceFullAccess
- AmazonElasticMapReducePlacementGroupPolicy
- AmazonElasticMapReduceReadOnlyAccess
- AmazonElasticMapReduceRole
- AmazonElasticsearchServiceRolePolicy
- AmazonElasticTranscoder_FullAccess
- AmazonElasticTranscoder_JobsSubmitter
- AmazonElasticTranscoder_ReadOnlyAccess
- AmazonElasticTranscoderRole
- AmazonEMRCleanupPolicy
- AmazonEMRContainersServiceRolePolicy
- AmazonEMRFullAccessPolicy_v2
- AmazonEMRReadOnlyAccessPolicy_v2
- AmazonEMRServerlessServiceRolePolicy
- AmazonEMRServicePolicy_v2

- AmazonEMRServicePolicyForSessions
- AmazonESCognitoAccess
- AmazonESFullAccess
- AmazonESReadOnlyAccess
- AmazonEventBridgeApiDestinationsServiceRolePolicy
- AmazonEventBridgeFullAccess
- AmazonEventBridgePipesFullAccess
- AmazonEventBridgePipesOperatorAccess
- AmazonEventBridgePipesReadOnlyAccess
- AmazonEventBridgeReadOnlyAccess
- AmazonEventBridgeSchedulerFullAccess
- AmazonEventBridgeSchedulerReadOnlyAccess
- AmazonEventBridgeSchemasFullAccess
- AmazonEventBridgeSchemasReadOnlyAccess
- AmazonEventBridgeSchemasServiceRolePolicy
- AmazonEVSServiceRolePolicy
- AmazonFISServiceRolePolicy
- AmazonForecastFullAccess
- AmazonFraudDetectorFullAccessPolicy
- AmazonFreeRTOSFullAccess
- AmazonFreeRTOSOTAUpdate
- AmazonFSxConsoleFullAccess
- AmazonFSxConsoleReadOnlyAccess
- AmazonFSxFullAccess
- AmazonFSxReadOnlyAccess
- AmazonFSxServiceRolePolicy
- AmazonGlacierFullAccess
- AmazonGlacierReadOnlyAccess
- AmazonGrafanaAthenaAccess

- AmazonGrafanaCloudWatchAccess
- AmazonGrafanaRedshiftAccess
- AmazonGrafanaServiceLinkedRolePolicy
- AmazonGuardDutyFullAccess
- AmazonGuardDutyFullAccess_v2
- AmazonGuardDutyMalwareProtectionServiceRolePolicy
- AmazonGuardDutyReadOnlyAccess
- AmazonGuardDutyServiceRolePolicy
- AmazonHealthLakeFullAccess
- AmazonHealthLakeReadOnlyAccess
- AmazonHoneycodeFullAccess
- AmazonHoneycodeReadOnlyAccess
- AmazonHoneycodeServiceRolePolicy
- AmazonHoneycodeTeamAssociationFullAccess
- AmazonHoneycodeTeamAssociationReadOnlyAccess
- AmazonHoneycodeWorkbookFullAccess
- AmazonHoneycodeWorkbookReadOnlyAccess
- AmazonInspector2AgentlessServiceRolePolicy
- AmazonInspector2AmiScanServiceRolePolicy
- AmazonInspector2FullAccess
- AmazonInspector2FullAccess_v2
- AmazonInspector2ManagedCisPolicy
- AmazonInspector2ManagedTelemetryPolicy
- AmazonInspector2ReadOnlyAccess
- AmazonInspector2ServiceRolePolicy
- AmazonInspector2ThirdPartyServiceRolePolicy
- AmazonInspectorFullAccess
- AmazonInspectorReadOnlyAccess
- AmazonInspectorServiceRolePolicy

- AmazonKendraFullAccess
- AmazonKendraReadOnlyAccess
- AmazonKeyspacesFullAccess
- AmazonKeyspacesReadOnlyAccess
- AmazonKeyspacesReadOnlyAccess_v2
- AmazonKinesisAnalyticsFullAccess
- AmazonKinesisAnalyticsReadOnly
- AmazonKinesisFirehoseFullAccess
- AmazonKinesisFirehoseReadOnlyAccess
- AmazonKinesisFullAccess
- AmazonKinesisReadOnlyAccess
- AmazonKinesisVideoStreamsFullAccess
- AmazonKinesisVideoStreamsReadOnlyAccess
- AmazonLaunchWizard_Akses Penuh
- AmazonLaunchWizardFullAccessV2
- AmazonLexChannelsAccess
- AmazonLexFullAccess
- AmazonLexReadOnly
- AmazonLexReplicationPolicy
- AmazonLexRunBotsOnly
- AmazonLexV2BotPolicy
- AmazonLookoutEquipmentFullAccess
- AmazonLookoutEquipmentReadOnlyAccess
- AmazonLookoutMetricsFullAccess
- AmazonLookoutMetricsReadOnlyAccess
- AmazonLookoutVisionConsoleFullAccess
- AmazonLookoutVisionConsoleReadOnlyAccess
- AmazonLookoutVisionFullAccess
- AmazonLookoutVisionReadOnlyAccess

- AmazonMachineLearningBatchPredictionsAccess
- AmazonMachineLearningCreateOnlyAccess
- AmazonMachineLearningFullAccess
- AmazonMachineLearningManageRealTimeEndpointOnlyAccess
- AmazonMachineLearningReadOnlyAccess
- AmazonMachineLearningRealTimePredictionOnlyAccess
- AmazonMachineLearningRoleforRedshiftDataSourceV3
- AmazonMacieFullAccess
- AmazonMacieHandshakeRole
- AmazonMacieReadOnlyAccess
- AmazonMacieServiceRole
- AmazonMacieServiceRolePolicy
- AmazonManagedBlockchainConsoleFullAccess
- AmazonManagedBlockchainFullAccess
- AmazonManagedBlockchainReadOnlyAccess
- AmazonManagedBlockchainServiceRolePolicy
- AmazonMCSFullAccess
- AmazonMCSReadOnlyAccess
- AmazonMechanicalTurkFullAccess
- AmazonMechanicalTurkReadOnly
- AmazonMemoryDBFullAccess
- AmazonMemoryDBReadOnlyAccess
- AmazonMobileAnalyticsFinancialReportAccess
- AmazonMobileAnalyticsFullAccess
- AmazonMobileAnalyticsNon-financialReportAccess
- AmazonMobileAnalyticsWriteOnlyAccess
- AmazonMonitronFullAccess
- AmazonMQApiFullAccess
- AmazonMQApiReadOnlyAccess

- AmazonMQFullAccess
- AmazonMQReadOnlyAccess
- AmazonMQServiceRolePolicy
- AmazonMSKConnectReadOnlyAccess
- AmazonMSKFullAccess
- AmazonMSKReadOnlyAccess
- AmazonMWAAServerlessServiceRolePolicy
- AmazonMWAAServiceRolePolicy
- AmazonNimbleStudio-LaunchProfileWorker
- AmazonNimbleStudio-StudioAdmin
- AmazonNimbleStudio-StudioUser
- AmazonODBAutonomousDatabaseAdmin
- AmazonODBAutonomousVmClusterAdmin
- AmazonODBExadataInfrastructureAdmin
- AmazonODBExadataVmClusterAdmin
- AmazonODBExascaleStorageVaultAdmin
- AmazonODBExascaleVmClusterAdmin
- AmazonODBFullAccess
- AmazonODBNetworkAdmin
- AmazonODBReadOnlyAccess
- AmazonODBServiceRolePolicy
- AmazonOmicsFullAccess
- AmazonOmicsReadOnlyAccess
- AmazonOneEnterpriseFullAccess
- AmazonOneEnterpriseInstallerAccess
- AmazonOneEnterpriseReadOnlyAccess
- AmazonOpenSearchDashboardsServiceRolePolicy
- AmazonOpenSearchDirectQueryGlueCreateAccess
- AmazonOpenSearchIngestionFullAccess

- AmazonOpenSearchIngestionReadOnlyAccess
- AmazonOpenSearchIngestionServiceRolePolicy
- AmazonOpenSearchServerlessServiceRolePolicy
- AmazonOpenSearchServiceCognitoAccess
- AmazonOpenSearchServiceFullAccess
- AmazonOpenSearchServiceReadOnlyAccess
- AmazonOpenSearchServiceRolePolicy
- AmazonPersonalizeFullAccess
- AmazonPollyFullAccess
- AmazonPollyReadOnlyAccess
- AmazonPrometheusConsoleFullAccess
- AmazonPrometheusFullAccess
- AmazonPrometheusQueryAccess
- AmazonPrometheusRemoteWriteAccess
- AmazonPrometheusScraperServiceRolePolicy
- AmazonQDeveloperAccess
- AmazonQFullAccess
- AmazonQLDBConsoleFullAccess
- AmazonQLDBFullAccess
- AmazonQLDBReadOnly
- AmazonRDSBetaServiceRolePolicy
- AmazonRDSCustomInstanceProfileRolePolicy
- AmazonRDSCustomPreviewServiceRolePolicy
- AmazonRDSCustomServiceRolePolicy
- AmazonRDSDataFullAccess
- AmazonRDSDirectoryServiceAccess
- AmazonRDSEnhancedMonitoringRole
- AmazonRDSFullAccess
- AmazonRDSPerformanceInsightsFullAccess

- AmazonRDSPerformanceInsightsReadOnly
- AmazonRDSPreviewServiceRolePolicy
- AmazonRDSReadOnlyAccess
- AmazonRDSServiceRolePolicy
- AmazonRedshiftAllCommandsFullAccess
- AmazonRedshiftDataFullAccess
- AmazonRedshiftFederatedAuthorization
- AmazonRedshiftFullAccess
- AmazonRedshiftQueryEditor
- AmazonRedshiftQueryEditorV2FullAccess
- AmazonRedshiftQueryEditorV2NoSharing
- AmazonRedshiftQueryEditorV2ReadSharing
- AmazonRedshiftQueryEditorV2ReadWriteSharing
- AmazonRedshiftReadOnlyAccess
- AmazonRedshiftServiceLinkedRolePolicy
- AmazonRekognitionCustomLabelsFullAccess
- AmazonRekognitionFullAccess
- AmazonRekognitionReadOnlyAccess
- AmazonRekognitionServiceRole
- AmazonRoute53AutoNamingFullAccess
- AmazonRoute53AutoNamingReadOnlyAccess
- AmazonRoute53AutoNamingRegistrantAccess
- AmazonRoute53DomainsFullAccess
- AmazonRoute53DomainsReadOnlyAccess
- AmazonRoute53FullAccess
- AmazonRoute53GlobalResolverFullAccess
- AmazonRoute53GlobalResolverReadOnlyAccess
- AmazonRoute53ProfilesFullAccess
- AmazonRoute53ProfilesReadOnlyAccess

- AmazonRoute53ReadOnlyAccess
- AmazonRoute53RecoveryClusterFullAccess
- AmazonRoute53RecoveryClusterReadOnlyAccess
- AmazonRoute53RecoveryControlConfigFullAccess
- AmazonRoute53RecoveryControlConfigReadOnlyAccess
- AmazonRoute53RecoveryReadinessFullAccess
- AmazonRoute53RecoveryReadinessReadOnlyAccess
- AmazonRoute53ResolverFullAccess
- AmazonRoute53ResolverReadOnlyAccess
- AmazonS3ExpressFullAccess
- AmazonS3ExpressReadOnlyAccess
- AmazonS3FilesClientFullAccess
- AmazonS3FilesClientReadOnlyAccess
- AmazonS3FilesClientReadWriteAccess
- AmazonS3FilesCSIDriverPolicy
- AmazonS3FilesFullAccess
- AmazonS3FilesReadOnlyAccess
- AmazonS3FullAccess
- AmazonS3ObjectLambdaExecutionRolePolicy
- AmazonS3OutpostsFullAccess
- AmazonS3OutpostsReadOnlyAccess
- AmazonS3ReadOnlyAccess
- AmazonS3TablesFullAccess
- AmazonS3TablesLakeFormationServiceRole
- AmazonS3TablesReadOnlyAccess
- AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy
- AmazonSageMakerCanvasAIServicesAccess
- AmazonSageMakerCanvasBedrockAccess
- AmazonSageMakerCanvasDataPrepFullAccess

- AmazonSageMakerCanvasDirectDeployAccess
- AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy
- AmazonSageMakerCanvasForecastAccess
- AmazonSageMakerCanvasFullAccess
- AmazonSageMakerCanvasSMDataScienceAssistantAccess
- AmazonSageMakerCapacityReservationServiceRolePolicy
- AmazonSageMakerClusterInstanceRolePolicy
- AmazonSageMakerCoreServiceRolePolicy
- AmazonSageMakerEdgeDeviceFleetPolicy
- AmazonSageMakerFeatureStoreAccess
- AmazonSageMakerFullAccess
- AmazonSageMakerGeospatialExecutionRole
- AmazonSageMakerGeospatialFullAccess
- AmazonSageMakerGroundTruthExecution
- AmazonSageMakerHyperPodGatedModelAccess
- AmazonSageMakerHyperPodInferenceAccess
- AmazonSageMakerHyperPodInferenceGatewayAccess
- AmazonSageMakerHyperPodObservabilityAdminAccess
- AmazonSageMakerHyperPodServiceRolePolicy
- AmazonSageMakerHyperPodTrainingOperatorAccess
- AmazonSageMakerInferenceServiceRolePolicy
- AmazonSageMakerJobFullAccess
- AmazonSageMakerJobRuntimeAccess
- AmazonSageMakerMechanicalTurkAccess
- AmazonSageMakerModelCustomizationCoreAccess
- AmazonSageMakerModelGovernanceUseAccess
- AmazonSageMakerModelRegistryFullAccess
- AmazonSageMakerNotebooksServiceRolePolicy
- AmazonSageMakerPartnerAppsFullAccess

- AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy
- AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy
- AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy
- AmazonSageMakerPipelinesIntegrations
- AmazonSageMakerQuickSightVPCPolicy
- AmazonSageMakerReadOnly
- AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy
- AmazonSageMakerSpacesControllerPolicy
- AmazonSageMakerSpacesRouterPolicy
- AmazonSageMakerTrainingPlanCreateAccess
- AmazonSecurityLakeAdministrator
- AmazonSecurityLakeMetastoreManager
- AmazonSecurityLakePermissionsBoundary
- AmazonSESFullAccess
- AmazonSESReadOnlyAccess
- AmazonSESServiceRolePolicy
- AmazonSNSFullAccess
- AmazonSNSReadOnlyAccess
- AmazonsnsPeran
- AmazonSQSFullAccess
- AmazonSQSReadOnlyAccess
- AmazonSSMAutomationApproverAccess

- AmazonSSMAutomationRole
- AmazonSSMDirectoryServiceAccess
- AmazonSSMFullAccess
- AmazonSSMMaintenanceWindowRole
- AmazonSSMManagedEC2InstanceDefaultPolicy
- AmazonSSMManagedInstanceCore
- AmazonSSMPatchAssociation
- AmazonSSMReadOnlyAccess
- AmazonSSMServiceRolePolicy
- AmazonSumerianFullAccess
- AmazonTextractFullAccess
- AmazonTextractServiceRole
- AmazonTimestreamConsoleFullAccess
- AmazonTimestreamFullAccess
- AmazonTimestreamInfluxDBFullAccess
- AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess
- AmazonTimestreamInfluxDBServiceRolePolicy
- AmazonTimestreamReadOnlyAccess
- AmazonTranscribeFullAccess
- AmazonTranscribeReadOnlyAccess
- AmazonVerifiedPermissionsFullAccess
- AmazonVerifiedPermissionsReadOnlyAccess
- AmazonVPCCrossAccountNetworkInterfaceOperations
- AmazonVPCFullAccess
- AmazonVPCNetworkAccessAnalyzerFullAccessPolicy
- AmazonVPCReachabilityAnalyzerFullAccessPolicy
- AmazonVPCReachabilityAnalyzerPathComponentReadPolicy
- AmazonVPCReadOnlyAccess
- AmazonWorkDocsFullAccess

- AmazonWorkDocsReadOnlyAccess
- AmazonWorkMailEventsServiceRolePolicy
- AmazonWorkMailFullAccess
- AmazonWorkMailMessageFlowFullAccess
- AmazonWorkMailMessageFlowReadOnlyAccess
- AmazonWorkMailReadOnlyAccess
- AmazonWorkSpacesAdmin
- AmazonWorkSpacesApplicationManagerAdminAccess
- AmazonWorkspacesPCAAccess
- AmazonWorkSpacesPoolServiceAccess
- AmazonWorkSpacesSecureBrowserReadOnly
- AmazonWorkSpacesSelfServiceAccess
- AmazonWorkSpacesServiceAccess
- AmazonWorkSpacesThinClientFullAccess
- AmazonWorkSpacesThinClientMonitoringServiceRolePolicy
- AmazonWorkSpacesThinClientReadOnlyAccess
- AmazonWorkSpacesWebReadOnly
- AmazonWorkSpacesWebServiceRolePolicy
- AmazonZocaloFullAccess
- AmazonZocaloReadOnlyAccess
- AmplifyBackendDeployFullAccess
- AnthropicFullAccess
- AnthropicLimitedAccess
- AnthropicReadOnlyAccess
- AnthropicSelfHostedEnvironmentAccess
- APIGatewayServiceRolePolicy
- AppIntegrationsServiceLinkedRolePolicy
- ApplicationAutoScalingForAmazonAppStreamAccess
- ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

- AppRunnerNetworkingServiceRolePolicy
- AppRunnerServiceRolePolicy
- AppStudioServiceRolePolicy
- AssuranceServiceRolePolicy
- AuroraDsqlServiceLinkedRolePolicy
- AutoScalingConsoleFullAccess
- AutoScalingConsoleReadOnlyAccess
- AutoScalingFullAccess
- AutoScalingNotificationAccessRole
- AutoScalingReadOnlyAccess
- AutoScalingServiceRolePolicy
- AWS-SSM-Automation-DiagnosisBucketPolicy
- AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy
- AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy
- AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy
- AWS-SSM-RemediationAutomation-AdministrationRolePolicy
- AWS-SSM-RemediationAutomation-ExecutionRolePolicy
- AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy
- AWS_ ConfigRole
- AWSAccountActivityAccess
- AWSAccountManagementFullAccess
- AWSAccountManagementReadOnlyAccess
- AWSAccountSettingsManagementRole
- AWSAccountUsageReportAccess
- AWSAgentlessDiscoveryService
- AWSAgentRegistryServiceRolePolicy
- AWSAppConfigServiceRolePolicy
- AWSAppFabricFullAccess
- AWSAppFabricReadOnlyAccess

- AWSAppFabricServiceRolePolicy
- AWSApplicationAutoscalingAppStreamFleetPolicy
- AWSApplicationAutoscalingCassandraTablePolicy
- AWSApplicationAutoscalingComprehendEndpointPolicy
- AWSApplicationAutoScalingCustomResourcePolicy
- AWSApplicationAutoscalingDynamoDBTablePolicy
- AWSApplicationAutoscalingEC2SpotFleetRequestPolicy
- AWSApplicationAutoscalingECSServicePolicy
- AWSApplicationAutoscalingElastiCacheRGPolicy
- AWSApplicationAutoscalingEMRInstanceGroupPolicy
- AWSApplicationAutoscalingKafkaClusterPolicy
- AWSApplicationAutoscalingLambdaConcurrencyPolicy
- AWSApplicationAutoscalingNeptuneClusterPolicy
- AWSApplicationAutoscalingRDSClusterPolicy
- AWSApplicationAutoscalingSageMakerEndpointPolicy
- AWSApplicationAutoscalingWorkSpacesPoolPolicy
- AWSApplicationDiscoveryAgentAccess
- AWSApplicationDiscoveryAgentlessCollectorAccess
- AWSApplicationDiscoveryServiceFullAccess
- AWSApplicationMigrationAgentInstallationPolicy
- AWSApplicationMigrationAgentPolicy
- AWSApplicationMigrationAgentPolicy_v2
- AWSApplicationMigrationConversionServerPolicy
- AWSApplicationMigrationEC2Access
- AWSApplicationMigrationFSxProxyPolicy
- AWSApplicationMigrationFSxProxyVPCPolicy
- AWSApplicationMigrationFullAccess
- AWSApplicationMigrationMGHAccess
- AWSApplicationMigrationNetworkMigrationCustomResource

- AWSApplicationMigrationNetworkMigrationMultiAccount
- AWSApplicationMigrationReadOnlyAccess
- AWSApplicationMigrationReplicationServerPolicy
- AWSApplicationMigrationServiceEc2InstancePolicy
- AWSApplicationMigrationServiceRolePolicy
- AWSApplicationMigrationSSMAccess
- AWSApplicationMigrationVCenterClientPolicy
- AWSAppMeshEnvoyAccess
- AWSAppMeshFullAccess
- AWSAppMeshPreviewEnvoyAccess
- AWSAppMeshPreviewServiceRolePolicy
- AWSAppMeshReadOnly
- AWSAppMeshServiceRolePolicy
- AWSAppRunnerFullAccess
- AWSAppRunnerReadOnlyAccess
- AWSAppRunnerServicePolicyForECRAccess
- AWSAppSyncAdministrator
- AWSAppSyncInvokeFullAccess
- AWSAppSyncPushToCloudWatchLogs
- AWSAppSyncSchemaAuthor
- AWSAppSyncServiceRolePolicy
- AWSArtifactAccountSync
- AWSArtifactAgreementsFullAccess
- AWSArtifactAgreementsReadOnlyAccess
- AWSArtifactComplianceInquiriesFullAccess
- AWSArtifactComplianceInquiriesReadOnlyAccess
- AWSArtifactReportsReadOnlyAccess
- AWSArtifactServiceRolePolicy
- AWSAuditManagerAdministratorAccess

- AWSAuditManagerServiceRolePolicy
- AWSAutoScalingPlansEC2AutoScalingPolicy
- AWSBackupAccessPointOperatorAccess
- AWSBackupAuditAccess
- AWSBackupDataTransferAccess
- AWSBackupFullAccess
- AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync
- AWSBackupGuardDutyRolePolicyForScans
- AWSBackupOperatorAccess
- AWSBackupOrganizationAdminAccess
- AWSBackupRestoreAccessForSAPHANA
- AWSBackupSearchOperatorAccess
- AWSBackupServiceLinkedRolePolicyForBackup
- AWSBackupServiceLinkedRolePolicyForBackupTest
- AWSBackupServiceRolePolicyForBackup
- AWSBackupServiceRolePolicyForIndexing
- AWSBackupServiceRolePolicyForItemRestores
- AWSBackupServiceRolePolicyForRestores
- AWSBackupServiceRolePolicyForS3Backup
- AWSBackupServiceRolePolicyForS3Restore
- AWSBackupServiceRolePolicyForScans
- AWSBatchFullAccess
- AWSBatchServiceEventTargetRole
- AWSBatchServiceRole
- AWSBatchServiceRolePolicyForSageMaker
- AWSBCMDataExportsServiceRolePolicy
- AWSBedrockAgentCoreGatewayNetworkServiceRolePolicy
- AWSBedrockAgentCoreIdentityNetworkServiceRolePolicy
- AWSBedrockAgentCoreRuntimeInstancesServiceRolePolicy

- AWSBillingConductorFullAccess
- AWSBillingConductorReadOnlyAccess
- AWSBillingConductorRolePolicy
- AWSBillingReadOnlyAccess
- AWSBillingServiceRolePolicy
- AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM
- AWSBudgetsActionsWithAWSResourceControlAccess
- AWSBudgetsReadOnlyAccess
- AWSBudgetsSpendLimitMemberRolePolicy
- AWSBugBustFullAccess
- AWSBugBustPlayerAccess
- AWSBugBustServiceRolePolicy
- AWSCertificateManagerFullAccess
- AWSCertificateManagerPrivateCAAuditor
- AWSCertificateManagerPrivateCAFullAccess
- AWSCertificateManagerPrivateCAPrivilegedUser
- AWSCertificateManagerPrivateCAReadOnly
- AWSCertificateManagerPrivateCAUser
- AWSCertificateManagerReadOnly
- AWSChatbotServiceLinkedRolePolicy
- AWSCleanRoomsFullAccess
- AWSCleanRoomsFullAccessNoQuerying
- AWSCleanRoomsMLFullAccess
- AWSCleanRoomsMLReadOnlyAccess
- AWSCleanRoomsReadOnlyAccess
- AWSCleanRoomsServiceRolePolicy
- AWSCloud9Administrator
- AWSCloud9EnvironmentMember
- AWSCloud9ServiceRolePolicy

- AWSCloud9SSMInstanceProfile
- AWSCloud9User
- AWSCloudFormationFullAccess
- AWSCloudFormationReadOnlyAccess
- AWSCloudFrontLogger
- AWSCloudFrontVPCOriginServiceRolePolicy
- AWSCloudHSMFullAccess
- AWSCloudHSMReadOnlyAccess
- AWSCloudHSMRole
- AWSCloudMapDiscoverInstanceAccess
- AWSCloudMapFullAccess
- AWSCloudMapReadOnlyAccess
- AWSCloudMapRegisterInstanceAccess
- AWSCloudShellFullAccess
- AWSCloudTrail_FullAccess
- AWSCloudTrail_ReadOnlyAccess
- AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy
- AWSCloudWatchOmniServiceRolePolicy
- AWSCodeArtifactAdminAccess
- AWSCodeArtifactReadOnlyAccess
- AWSCodeBuildAdminAccess
- AWSCodeBuildDeveloperAccess
- AWSCodeBuildReadOnlyAccess
- AWSCodeCommitFullAccess
- AWSCodeCommitPowerUser
- AWSCodeCommitReadOnly
- AWSCodeDeployDeployerAccess
- AWSCodeDeployFullAccess
- AWSCodeDeployReadOnlyAccess

- AWSCodeDeployRole
- AWSCodeDeployRoleForCloudFormation
- AWSCodeDeployRoleForECS
- AWSCodeDeployRoleForECSLimited
- AWSCodeDeployRoleForLambda
- AWSCodeDeployRoleForLambdaLimited
- AWSCodePipeline_FullAccess
- AWSCodePipeline_ReadOnlyAccess
- AWSCodePipelineApproverAccess
- AWSCodePipelineCustomActionAccess
- AWSCodeStarFullAccess
- AWSCodeStarNotificationsServiceRolePolicy
- AWSCodeStarServiceRole
- AWSCompromisedKeyQuarantine
- AWSCompromisedKeyQuarantineV2
- AWSCompromisedKeyQuarantineV3
- AWSConfigMultiAccountSetupPolicy
- AWSConfigRemediationServiceRolePolicy
- AWSConfigRoleForOrganizations
- AWSConfigRulesExecutionRole
- AWSConfigServiceRolePolicy
- AWSConfigThirdPartyServiceRolePolicy
- AWSConfigUserAccess
- Konektor AWS
- AWSControlTowerAccountServiceRolePolicy
- AWSControlTowerCloudTrailRolePolicy
- AWSControlTowerIdentityCenterManagementPolicy
- AWSControlTowerServiceRolePolicy
- AWSCostAndUsageReportAutomationPolicy

- AWSDataExchangeDataGrantOwnerFullAccess
- AWSDataExchangeDataGrantReceiverFullAccess
- AWSDataExchangeFullAccess
- AWSDataExchangeProviderFullAccess
- AWSDataExchangeReadOnly
- AWSDataExchangeServiceRolePolicyForLicenseManagement
- AWSDataExchangeServiceRolePolicyForOrganizationDiscovery
- AWSDataExchangeSubscriberFullAccess
- AWSDataLifecycleManagerServiceRole
- AWSDataLifecycleManagerServiceRoleForAMIManagement
- AWSDataLifecycleManagerSSMFullAccess
- AWSDataPipeline_FullAccess
- AWSDataPipeline_PowerUser
- AWSDataSyncDiscoveryServiceRolePolicy
- AWSDataSyncFullAccess
- AWSDataSyncReadOnlyAccess
- AWSDataSyncServiceRolePolicy
- AWSDeadlineCloud-FleetWorker
- AWSDeadlineCloud-UserAccessFarms
- AWSDeadlineCloud-UserAccessFleets
- AWSDeadlineCloud-UserAccessJobs
- AWSDeadlineCloud-UserAccessQueues
- AWSDeadlineCloud-WorkerHost
- AWSDeepLensLambdaFunctionAccessPolicy
- AWSDeepLensServiceRolePolicy
- AWSDeepRacerAccountAdminAccess
- AWSDeepRacerCloudFormationAccessPolicy
- AWSDeepRacerDefaultMultiUserAccess
- AWSDeepRacerFullAccess

- AWSDeepRacerRoboMakerAccessPolicy
- AWSDeepRacerServiceRolePolicy
- AWSDenyAll
- AWSDeviceFarmFullAccess
- AWSDeviceFarmServiceRolePolicy
- AWSDeviceFarmTestGridServiceRolePolicy
- AWSDirectConnectFullAccess
- AWSDirectConnectReadOnlyAccess
- AWSDirectConnectServiceRolePolicy
- AWSDirectoryServiceDataFullAccess
- AWSDirectoryServiceDataReadOnlyAccess
- AWSDirectoryServiceFullAccess
- AWSDirectoryServiceReadOnlyAccess
- AWSDirectoryServiceServiceRolePolicy
- AWSDiscoveryContinuousExportFirehosePolicy
- AWSDMSFleetAdvisorServiceRolePolicy
- AWSDMSServerlessServiceRolePolicy
- AWSEC2CapacityManagerServiceRolePolicy
- AWSEC2CapacityReservationFleetRolePolicy
- AWSEC2FleetServiceRolePolicy
- AWSEC2SpotFleetServiceRolePolicy
- AWSEC2SpotServiceRolePolicy
- AWSEC2SqlHaInstancePolicy
- AWSEC2SqlHaServiceRolePolicy
- AWSEC2VssRestorePolicy
- AWSEC2VssSnapshotPolicy
- AWSECRPullThroughCache_ServiceRolePolicy
- AWSElasticBeanstalkCustomPlatformforEC2Role
- AWSElasticBeanstalkEKSImageBuild
- AWSElasticBeanstalkEKSObservability

- AWSElasticBeanstalkEKSTagging
- AWSElasticBeanstalkEnhancedHealth
- AWSElasticBeanstalkMaintenance
- AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy
- AWSElasticBeanstalkManagedUpdatesServiceRolePolicy
- AWSElasticBeanstalkMulticontainerDocker
- AWSElasticBeanstalkReadOnly
- AWSElasticBeanstalkRoleCore
- AWSElasticBeanstalkRoleCWL
- AWSElasticBeanstalkRoleECS
- AWSElasticBeanstalkRoleRDS
- AWSElasticBeanstalkRoleSNS
- AWSElasticBeanstalkRoleWorkerTier
- AWSElasticBeanstalkService
- AWSElasticBeanstalkServiceRolePolicy
- AWSElasticBeanstalkWebTier
- AWSElasticBeanstalkWorkerTier
- AWSElasticDisasterRecoveryAgentInstallationPolicy
- AWSElasticDisasterRecoveryAgentPolicy
- AWSElasticDisasterRecoveryConsoleFullAccess
- AWSElasticDisasterRecoveryConsoleFullAccess_v2
- AWSElasticDisasterRecoveryConversionServerPolicy
- AWSElasticDisasterRecoveryCrossAccountReplicationPolicy
- AWSElasticDisasterRecoveryEc2InstancePolicy
- AWSElasticDisasterRecoveryFailbackInstallationPolicy
- AWSElasticDisasterRecoveryFailbackPolicy
- AWSElasticDisasterRecoveryLaunchActionsPolicy
- AWSElasticDisasterRecoveryNetworkReplicationPolicy
- AWSElasticDisasterRecoveryReadOnlyAccess
- AWSElasticDisasterRecoveryRecoveryInstancePolicy

- AWSElasticDisasterRecoveryReplicationServerPolicy
- AWSElasticDisasterRecoveryServiceRolePolicy
- AWSElasticDisasterRecoveryStagingAccountPolicy
- AWSElasticDisasterRecoveryStagingAccountPolicy_v2
- AWSElasticLoadBalancingClassicServiceRolePolicy
- AWSElasticLoadBalancingServiceRolePolicy
- AWSElementalMediaConnectCreateBridge
- AWSElementalMediaConnectCreateFlow
- AWSElementalMediaConnectDeleteBridge
- AWSElementalMediaConnectDeleteFlow
- AWSElementalMediaConnectFullAccess
- AWSElementalMediaConnectReadOnlyAccess
- AWSElementalMediaConvertFullAccess
- AWSElementalMediaConvertReadOnly
- AWSElementalMediaLiveFullAccess
- AWSElementalMediaLiveReadOnly
- AWSElementalMediaPackageFullAccess
- AWSElementalMediaPackageReadOnly
- AWSElementalMediaPackageV2FullAccess
- AWSElementalMediaPackageV2ReadOnly
- AWSElementalMediaStoreFullAccess
- AWSElementalMediaStoreReadOnly
- AWSElementalMediaTailorFullAccess
- AWSElementalMediaTailorReadOnly
- AWSEnhancedClassicNetworkingMangementPolicy
- AWSEntityResolutionConsoleFullAccess
- AWSEntityResolutionConsoleReadOnlyAccess
- AWSFaultInjectionSimulatorEC2Access
- AWSFaultInjectionSimulatorECSAccess
- AWSFaultInjectionSimulatorEKSAccess

- AWSFaultInjectionSimulatorNetworkAccess
- AWSFaultInjectionSimulatorRDSAccess
- AWSFaultInjectionSimulatorSSMAccess
- AWSFinSpaceServiceRolePolicy
- AWSFMAdminFullAccess
- AWSFMAdminReadOnlyAccess
- AWSFMMemberReadOnlyAccess
- AWSForWordPressPluginPolicy
- AWSGitSyncServiceRolePolicy
- AWSGlobalAcceleratorSLRPolicy
- AWSGlueConsoleFullAccess
- AWSGlueConsoleSageMakerNotebookFullAccess
- AwsGlueDataBrewFullAccessPolicy
- AWSGlueDataBrewServiceRole
- AWSGlueSchemaRegistryFullAccess
- AWSGlueSchemaRegistryReadonlyAccess
- AWSGlueServiceNotebookRole
- AWSGlueServiceRole
- AwsGlueSessionUserRestrictedNotebookPolicy
- AwsGlueSessionUserRestrictedNotebookServiceRole
- AwsGlueSessionUserRestrictedPolicy
- AwsGlueSessionUserRestrictedServiceRole
- AWSGrafanaAccountAdministrator
- AWSGrafanaConsoleReadOnlyAccess
- AWSGrafanaWorkspacePermissionManagement
- AWSGrafanaWorkspacePermissionManagementV2
- AWSGreengrassFullAccess
- AWSGreengrassReadOnlyAccess
- AWSGreengrassResourceAccessRolePolicy
- AWSGroundStationAgentInstancePolicy

- AWS Health_EventProcessorServiceRolePolicy
- AWSHealthFullAccess
- AWSHealthImagingFullAccess
- AWSHealthImagingReadOnlyAccess
- AWSHealthImagingServiceRolePolicy
- AWSHealthOmicsServiceLinkedRolePolicy
- AWSIAMIdentityCenterAllowListForIdentityContext
- AWSIAMRoleManagerServiceRolePolicy
- AWSIdentityCenterExternalManagementPolicy
- AWSIdentitySyncFullAccess
- AWSIdentitySyncReadOnlyAccess
- AWSImageBuilderFullAccess
- AWSImageBuilderReadOnlyAccess
- AWSImportExportFullAccess
- AWSImportExportReadOnlyAccess
- AWSIncidentManagerIncidentAccessServiceRolePolicy
- AWSIncidentManagerResolverAccess
- AWSIncidentManagerServiceRolePolicy
- AWSIoT1ClickFullAccess
- AWSIoT1ClickReadOnlyAccess
- AWSIoTAnalyticsFullAccess
- AWSIoTAnalyticsReadOnlyAccess
- AWSIoTConfigAccess
- AWSIoTConfigReadOnlyAccess
- AWSIoTDataAccess
- AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction
- AWSIoTDeviceDefenderAudit
- AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction
- AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction
- AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

- AWSIoTDeviceDefenderUpdateCACertMitigationAction
- AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction
- AWSIoTDeviceTesterForFreeRTOSFullAccess
- AWSIoTDeviceTesterForGreengrassFullAccess
- AWSIoTEventsFullAccess
- AWSIoTEventsReadOnlyAccess
- AWSIoTFleetHubFederationAccess
- AWSIoTFleetwiseServiceRolePolicy
- AWSIoTFullAccess
- AWSIoTLogging
- AWSIoTManagedIntegrationsFullAccess
- AWSIoTManagedIntegrationsRolePolicy
- AWSIoTOTAUpdate
- AWSIotRoboRunnerFullAccess
- AWSIotRoboRunnerReadOnly
- AWSIotRoboRunnerServiceRolePolicy
- AWSIoTRuleActions
- AWSIoTSiteWiseConsoleFullAccess
- AWSIoTSiteWiseFullAccess
- AWSIoTSiteWiseMonitorPortalAccess
- AWSIoTSiteWiseMonitorServiceRolePolicy
- AWSIoTSiteWiseReadOnlyAccess
- AWSIoTThingsRegistration
- AWSIoTTwinMakerServiceRolePolicy
- AWSIoTWirelessDataAccess
- AWSIoTWirelessFullAccess
- AWSIoTWirelessFullPublishAccess
- AWSIoTWirelessGatewayCertManager
- AWSIoTWirelessLogging
- AWSIoTWirelessReadOnlyAccess

- AWSIPAMServiceRolePolicy
- AWSIQContractServiceRolePolicy
- AWSIQFullAccess
- AWSIQPermissionServiceRolePolicy
- AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy
- AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy
- AWSKeyManagementServicePowerUser
- AWSLakeFormationCrossAccountManager
- AWSLakeFormationDataAdmin
- AWS Lambda_FullAccess
- AWS Lambda_ReadOnlyAccess
- AWSLambdaBasicDurableExecutionRolePolicy
- AWSLambdaBasicExecutionRole
- AWSLambdaDynamoDBExecutionRole
- AWSLambdaENIManagementAccess
- AWSLambdaExecute
- AWSLambdaFullAccess
- AWSLambdaInvocation-DynamoDB
- AWSLambdaInvokeWebFunctionEndpointAccess
- AWSLambdaKinesisExecutionRole
- AWSLambdaManagedEC2ResourceOperator
- AWSLambdaMSKExecutionRole
- AWSLambdaNetworkConnectorOperatorPolicy
- AWSLambdaReplicator
- AWSLambdaRole
- AWSLambdaServiceRolePolicy
- AWSLambdaSQSQueueExecutionRole
- AWSLambdaVPCAccessExecutionRole
- AWSLicenseManagerConsumptionPolicy
- AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

- AWSLicenseManagerMasterAccountRolePolicy
- AWSLicenseManagerMemberAccountRolePolicy
- AWSLicenseManagerServiceRolePolicy
- AWSLicenseManagerUserSubscriptionsServiceRolePolicy
- AWSM2ServicePolicy
- AWSManagedAccountManagementAccess
- AWSManagedAccountUserEntitlementAccess
- AWSManagedAdvancedFeaturesActivationAccess
- AWSManagedBudgetsSpendLimitManagementAccess
- AWSManagedControlPolicyManagementAccess
- AWSManagedServiceAccessManagementAccess
- AWSManagedServices_ContactsServiceRolePolicy
- AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy
- AWSManagedServices_EventsServiceRolePolicy
- AWSManagedServices_SelfServiceReporting_ServiceRolePolicy
- AWSManagedServicesDeploymentToolkitPolicy
- AWSManagedSettingsAdminAccess
- AWSManagedSettingsReadOnlyAccess
- AWSManagedSignUpAdminAccess
- AWSManagementConsoleAdministratorAccess
- AWSManagementConsoleBasicUserAccess
- AWSMarketplaceAmiIngestion
- AWSMarketplaceDeploymentServiceRolePolicy
- AWSMarketplaceDiscoveryFullAccess
- AWSMarketplaceFullAccess
- AWSMarketplaceGetEntitlements
- AWSMarketplaceImageBuildFullAccess
- AWSMarketplaceLicenseManagementServiceRolePolicy
- AWSMarketplaceManageSubscriptions
- AWSMarketplaceMeteringFullAccess

- AWSMarketplaceMeteringRegisterUsage
- AWSMarketplaceProcurementSystemAdminFullAccess
- AWSMarketplacePurchaseOrdersServiceRolePolicy
- AWSMarketplaceRead-only
- AWSMarketplaceResaleAuthorizationServiceRolePolicy
- AWSMarketplaceSellerFullAccess
- AWSMarketplaceSellerOfferManagement
- AWSMarketplaceSellerProductsFullAccess
- AWSMarketplaceSellerProductsReadOnly
- AWSMcpServiceActionsFullAccess
- AWSMCPSignInOAuthAccessPolicy
- AWSMediaConnectServicePolicy
- AWSMediaLiveAnywhereServiceRolePolicy
- AWSMediaTailorServiceRolePolicy
- AWSMigrationHubDiscoveryAccess
- AWSMigrationHubDMSAccess
- AWSMigrationHubFullAccess
- AWSMigrationHubOrchestratorConsoleFullAccess
- AWSMigrationHubOrchestratorInstanceRolePolicy
- AWSMigrationHubOrchestratorPlugin
- AWSMigrationHubOrchestratorServiceRolePolicy
- AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess
- AWSMigrationHubRefactorSpaces-SSMAutomationPolicy
- AWSMigrationHubRefactorSpacesFullAccess
- AWSMigrationHubRefactorSpacesServiceRolePolicy
- AWSMigrationHubSMSAccess
- AWSMigrationHubStrategyCollector
- AWSMigrationHubStrategyConsoleFullAccess
- AWSMigrationHubStrategyServiceRolePolicy
- AWSMobileHub_FullAccess

- AWSMobileHub_ReadOnly
- AWSMSKReplicatorExecutionRole
- AWSNATGatewayServiceRolePolicy
- AWSNetworkFirewallFullAccess
- AWSNetworkFirewallReadOnlyAccess
- AWSNetworkFirewallServiceRolePolicy
- AWSNetworkManagerCloudWANServiceRolePolicy
- AWSNetworkManagerFullAccess
- AWSNetworkManagerReadOnlyAccess
- AWSNetworkManagerServiceRolePolicy
- AWSObservabilityAdminLogsCentralizationServiceRolePolicy
- AWSObservabilityAdminServiceRolePolicy
- AWSObservabilityAdminTelemetryEnablementServiceRolePolicy
- AWSOrganizationsFullAccess
- AWSOrganizationsReadOnlyAccess
- AWSOrganizationsServiceTrustPolicy
- AWSOutpostsAuthorizeServerPolicy
- AWSOutpostsServiceRolePolicy
- AWSPanoramaApplianceRolePolicy
- AWSPanoramaApplianceServiceRolePolicy
- AWSPanoramaFullAccess
- AWSPanoramaGreengrassGroupRolePolicy
- AWSPanoramaSageMakerRolePolicy
- AWSPanoramaServiceLinkedRolePolicy
- AWSPanoramaServiceRolePolicy
- AWSPartnerCentralChannelHandshakeApprovalManagement
- AWSPartnerCentralChannelManagement
- AWSPartnerCentralFullAccess
- AWSPartnerCentralMarketingManagement
- AWSPartnerCentralOpportunityManagement

- AWSPartnerCentralRevenueAttributionManagement
- AWSPartnerCentralSandboxFullAccess
- AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy
- AWSPartnerLedSupportReadOnlyAccess
- AWSPartnerProServeToolsFullAccess
- AWSPartnerProServeToolsIndividualContributor
- AWSPartnerProServeToolsOrganizationReaderIndividualContributor
- AWSPCSComputeNodePolicy
- AWSPCSServiceRolePolicy
- AWSPriceListServiceFullAccess
- AWSPrivateCAAuditor
- AWSPrivateCAConnectorForKubernetesPolicy
- AWSPrivateCAFullAccess
- AWSPrivateCAPrivilegedUser
- AWSPrivateCAReadOnly
- AWSPrivateCAUser
- AWSPrivateMarketplaceAdminFullAccess
- AWSPrivateMarketplaceRequests
- AWSPrivateNetworksServiceRolePolicy
- AWSProtonCodeBuildProvisioningBasicAccess
- AWSProtonCodeBuildProvisioningServiceRolePolicy
- AWSProtonDeveloperAccess
- AWSProtonFullAccess
- AWSProtonReadOnlyAccess
- AWSProtonServiceGitSyncServiceRolePolicy
- AWSProtonSyncServiceRolePolicy
- AWSPurchaseOrdersServiceRolePolicy
- AWSQuickSetupCFGCPacksPermissionsBoundary
- AWSQuickSetupDeploymentRolePolicy
- AWSQuickSetupDevOpsGuruPermissionsBoundary

- AWSQuickSetupDistributorPermissionsBoundary
- AWSQuickSetupEnableAREXExecutionPolicy
- AWSQuickSetupEnableDHMCExecutionPolicy
- AWSQuickSetupJITNADeploymentRolePolicy
- AWSQuickSetupManagedInstanceProfileExecutionPolicy
- AWSQuickSetupManageJITNAResourcesExecutionPolicy
- AWSQuickSetupPatchPolicyBaselineAccess
- AWSQuickSetupPatchPolicyDeploymentRolePolicy
- AWSQuickSetupPatchPolicyLambdaExecutionPolicy
- AWSQuickSetupPatchPolicyPermissionsBoundary
- AWSQuickSetupPatchPolicyTagManagementExecutionPolicy
- AWSQuickSetupSchedulerPermissionsBoundary
- AWSQuickSetupSSMDeploymentRolePolicy
- AWSQuickSetupSSMDeploymentS3BucketRolePolicy
- AWSQuickSetupSSMHostMgmtPermissionsBoundary
- AWSQuickSetupSSMLifecycleManagementExecutionPolicy
- AWSQuickSetupSSMManageResourcesExecutionPolicy
- AWSQuickSetupStartSSMAssociationsExecutionPolicy
- AWSQuickSetupStartStopInstancesExecutionPolicy
- AWSQuickSightAssetBundleExportPolicy
- AWSQuickSightAssetBundleImportPolicy
- AWSQuicksightAthenaAccess
- AWSQuickSightDescribeRDS
- AWSQuickSightDescribeRedshift
- AWSQuickSightElasticsearchPolicy
- AWSQuickSightIoTAnalyticsAccess
- AWSQuickSightListIAM
- AWSQuicksightOpenSearchPolicy
- AWSQuickSightSageMakerPolicy
- AWSQuickSightSecretsManagerWriteAccess

- AWSQuickSightSecretsManagerWritePolicy
- AWSQuickSightTimestreamPolicy
- AWSReachabilityAnalyzerServiceRolePolicy
- AWSRefactoringToolkitFullAccess
- AWSRefactoringToolkitSidecarPolicy
- AWSrePostPrivateCloudWatchAccess
- AWSRepostSpaceSupportOperationsPolicy
- AWSResilienceHubAsssessmentExecutionPolicy
- AWSResilienceHubResilienceTestingPolicy
- AWSResilienceHubServiceRolePolicy
- AWSResilienceHubV2AssessmentExecutionPolicy
- AWSResourceAccessManagerFullAccess
- AWSResourceAccessManagerReadOnlyAccess
- AWSResourceAccessManagerResourceShareParticipantAccess
- AWSResourceAccessManagerServiceRolePolicy
- AWSResourceExplorerFullAccess
- AWSResourceExplorerOrganizationsAccess
- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerServiceRolePolicy
- AWSResourceGroupsReadOnlyAccess
- AWSRevenueAttributionManagement
- AWSRoboMaker_FullAccess
- AWSRoboMakerReadOnlyAccess
- AWSRoboMakerServicePolicy
- AWSRoboMakerServiceRolePolicy
- AWSRolesAnywhereFullAccess
- AWSRolesAnywhereReadOnly
- AWSRolesAnywhereServicePolicy
- AWSS3OnOutpostsServiceRolePolicy
- AWSSavingsPlansFullAccess

- AWSSavingsPlansReadOnlyAccess
- AWSSDMPServiceRolePolicy
- AWSSecretsManagerClientReadOnlyAccess
- AWSSecurityAgentServiceRolePolicy
- AWSSecurityAgentWebAppPolicy
- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess
- AWSSecurityHubReadOnlyAccess
- AWSSecurityHubServiceRolePolicy
- AWSSecurityHubV2ServiceRolePolicy
- AWSSecurityIncidentResponseCaseFullAccess
- AWSSecurityIncidentResponseFullAccess
- AWSSecurityIncidentResponseReadOnlyAccess
- AWSSecurityIncidentResponseServiceRolePolicy
- AWSSecurityIncidentResponseTriageServiceRolePolicy
- AWSServiceCatalogAdminFullAccess
- AWSServiceCatalogAdminReadOnlyAccess
- AWSServiceCatalogAppRegistryFullAccess
- AWSServiceCatalogAppRegistryReadOnlyAccess
- AWSServiceCatalogAppRegistryServiceRolePolicy
- AWSServiceCatalogEndUserFullAccess
- AWSServiceCatalogEndUserReadOnlyAccess
- AWSServiceCatalogOrgsDataSyncServiceRolePolicy
- AWSServiceCatalogSyncServiceRolePolicy
- AWSServiceRoleForAIDevOpsPolicy
- AWSServiceRoleForAmazonEKSNodegroup
- AWSServiceRoleForAmazonQDeveloper
- AWSServiceRoleForAWSTransform
- AWSServiceRoleForAWSTransformCustom
- AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

- AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy
- AWSServiceRoleForCodeGuru-Profiler
- AWSServiceRoleForCodeWhispererPolicy
- AWSServiceRoleForEC2ScheduledInstances
- AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy
- AWSServiceRoleForImageBuilder
- AWSServiceRoleForIoTSiteWise
- AWSServiceRoleForLogDeliveryPolicy
- AWSServiceRoleForMonitronPolicy
- AWSServiceRoleForNeptuneGraphPolicy
- AWSServiceRoleForPrivateMarketplaceAdminPolicy
- AWSServiceRoleForProcurementInsightsPolicy
- AWSServiceRoleForSMS
- AWSServiceRoleForUserSubscriptions
- AWSServiceRolePolicyForBackupReports
- AWSServiceRolePolicyForBackupRestoreTesting
- AWSServiceRolePolicyForWorkspacesInstances
- AWSShieldDRTAccessPolicy
- AWSShieldServiceRolePolicy
- AWSSocialMessagingServiceRolePolicy
- AWSSSMForSAPServiceLinkedRolePolicy
- AWSSSMOpsInsightsServiceRolePolicy
- AWSSSODirectoryAdministrator
- AWSSSODirectoryReadOnly
- AWSSSOMasterAccountAdministrator
- AWSSSOMemberAccountAdministrator
- AWSSSOReadOnly
- AWSSSOServiceRolePolicy
- AWSStepFunctionsConsoleFullAccess
- AWSStepFunctionsFullAccess

- AWSStepFunctionsReadOnlyAccess
- AWSStorageGatewayFullAccess
- AWSStorageGatewayReadOnlyAccess
- AWSStorageGatewayServiceRolePolicy
- AWSSupplyChainFederationAdminAccess
- AWSSupportAccess
- AWSSupportAppFullAccess
- AWSSupportAppReadOnlyAccess
- AWSSupportPlansFullAccess
- AWSSupportPlansReadOnlyAccess
- AWSSupportPlansServiceRolePolicy
- AWSSupportServiceRolePolicy
- AWSSystemsManagerAccountDiscoveryServicePolicy
- AWSSystemsManagerChangeManagementServicePolicy
- AWSSystemsManagerEnableConfigRecordingExecutionPolicy
- AWSSystemsManagerEnableExplorerExecutionPolicy
- AWSSystemsManagerForSAPFullAccess
- AWSSystemsManagerForSAPReadOnlyAccess
- AWSSystemsManagerJustInTimeAccessServicePolicy
- AWSSystemsManagerJustInTimeAccessTokenPolicy
- AWSSystemsManagerJustInTimeAccessTokenSessionPolicy
- AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy
- AWSSystemsManagerNotificationsServicePolicy
- AWSSystemsManagerOpsDataSyncServiceRolePolicy
- AWSThinkboxAssetServerPolicy
- AWSThinkboxAWSPortalAdminPolicy
- AWSThinkboxAWSPortalGatewayPolicy
- AWSThinkboxAWSPortalWorkerPolicy
- AWSThinkboxDeadlineResourceTrackerAccessPolicy
- AWSThinkboxDeadlineResourceTrackerAdminPolicy

- AWSThinkboxDeadlineSpotEventPluginAdminPolicy
- AWSThinkboxDeadlineSpotEventPluginWorkerPolicy
- AWSTransferConsoleFullAccess
- AWSTransferFullAccess
- AWSTransferLoggingAccess
- AWSTransferReadOnlyAccess
- AWSTransferServiceRolePolicy
- AWSTransformApplicationDeploymentPolicy
- AWSTransformApplicationECSDeploymentPolicy
- AWSTransformCustomExecuteTransformations
- AWSTransformCustomFullAccess
- AWSTransformCustomManageTransformations
- AWSTransformInfrastructureExecutorAccessBatch
- AWSTransformInfrastructureExecutorAccessEC2
- AWSTransformLandingZoneAgentPolicy
- AWSTransformNetworkMigrationAgentPolicy
- AWSTransformRevenueAttributionPolicy
- AWSTransformSecretsManagerConnectorPolicy
- AWSTransformSecurityAgentExecutorAccess
- AWSTransformServerMigrationAgentPolicy
- AWSTrustedAdvisorPriorityFullAccess
- AWSTrustedAdvisorPriorityReadOnlyAccess
- AWSTrustedAdvisorReportingServiceRolePolicy
- AWSTrustedAdvisorServiceRolePolicy
- AWSUserAttributeCostAllocationPolicy
- AWSUserNotificationsServiceLinkedRolePolicy
- AWSVendorInsightsAssessorFullAccess
- AWSVendorInsightsAssessorReadOnly
- AWSVendorInsightsVendorFullAccess
- AWSVendorInsightsVendorReadOnly

- AWSVPCFlowLogsServiceRolePolicy
- AWSVpcLatticeServiceRolePolicy
- AWSVPCS2SVpnServiceRolePolicy
- AWSVPCTransitGatewayServiceRolePolicy
- AWSVPCVerifiedAccessServiceRolePolicy
- AWSWAFConsoleFullAccess
- AWSWAFConsoleReadOnlyAccess
- AWSWAFFullAccess
- AWSWAFReadOnlyAccess
- AWSWellArchitectedAgentOrganizationsServiceRolePolicy
- AWSWellArchitectedAgentResourceScanningServiceRolePolicy
- AWSWellArchitectedDiscoveryServiceRolePolicy
- AWSWellArchitectedOrganizationsServiceRolePolicy
- AWSWickrFullAccess
- AWSXrayCrossAccountSharingConfiguration
- AWSXRayDaemonWriteAccess
- AWSXrayFullAccess
- AWSXrayReadOnlyAccess
- AWSXrayWriteOnlyAccess
- AWSZonalAutoshiftPracticeRunSLRPolicy
- AWSZoneGroupAccessManagementServiceRolePolicy
- BatchServiceRolePolicy
- BedrockAgentCoreFullAccess
- BedrockAgentCoreNetworkServiceRolePolicy
- BedrockAgentCoreRuntimeIdentityServiceRolePolicy
- BedrockAgentCoreRuntimeInstancesInstanceRolePolicy
- BedrockAgentCoreRuntimeInstancesOperatorRolePolicy
- Penagihan
- BudgetsServiceRolePolicy
- CertificateManagerServiceRolePolicy

- ClientVPNServiceConnectionsRolePolicy
- ClientVPNServiceRolePolicy
- CloudFormationStackSetsOrgAdminServiceRolePolicy
- CloudFormationStackSetsOrgMemberServiceRolePolicy
- CloudFrontFullAccess
- CloudFrontReadOnlyAccess
- CloudHSMServiceRolePolicy
- CloudSearchFullAccess
- CloudSearchReadOnlyAccess
- CloudTrailEventContext
- CloudTrailServiceRolePolicy
- CloudWatch-CrossAccountAccess
- CloudWatchActionsEC2Access
- CloudWatchAgentAdminPolicy
- CloudWatchAgentServerPolicy
- CloudWatchAPIKeyAccess
- CloudWatchApplicationInsightsFullAccess
- CloudWatchApplicationInsightsReadOnlyAccess
- CloudwatchApplicationInsightsServiceLinkedRolePolicy
- CloudWatchApplicationSignalsFullAccess
- CloudWatchApplicationSignalsReadOnlyAccess
- CloudWatchApplicationSignalsServiceRolePolicy
- CloudWatchAutomaticDashboardsAccess
- CloudWatchCrossAccountSharingConfiguration
- CloudWatchEventsBuiltInTargetExecutionAccess
- CloudWatchEventsFullAccess
- CloudWatchEventsInvocationAccess
- CloudWatchEventsReadOnlyAccess
- CloudWatchEventsServiceRolePolicy
- CloudWatchFullAccess

- CloudWatchFullAccessV2
- CloudWatchInternetMonitorFullAccess
- CloudWatchInternetMonitorReadOnlyAccess
- CloudWatchInternetMonitorServiceRolePolicy
- CloudWatchLambdaApplicationSignalsExecutionRolePolicy
- CloudWatchLambdaInsightsExecutionRolePolicy
- CloudWatchLogsAPIKeyAccess
- CloudWatchLogsCrossAccountSharingConfiguration
- CloudWatchLogsFullAccess
- CloudWatchLogsReadOnlyAccess
- CloudWatchNetworkFlowMonitorAgentPublishPolicy
- CloudWatchNetworkFlowMonitorServiceRolePolicy
- CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy
- CloudWatchNetworkMonitorServiceRolePolicy
- CloudWatchOmniAWSIntegrationPolicy
- CloudWatchOmniDomainAccessPolicy
- CloudWatchOmniModelInferencePolicy
- CloudWatchOmniSpaceAccessPolicy
- CloudWatchOpenSearchDashboardAccess
- CloudWatchOpenSearchDashboardsFullAccess
- CloudWatchReadOnlyAccess
- CloudWatchSyntheticsFullAccess
- CloudWatchSyntheticsReadOnlyAccess
- ComprehendDataAccessRolePolicy
- ComprehendFullAccess
- ComprehendMedicalFullAccess
- ComprehendReadOnly
- ComputeOptimizerAutomationServiceRolePolicy
- ComputeOptimizerReadOnlyAccess
- ComputeOptimizerServiceRolePolicy

- ConfigConformsServiceRolePolicy
- ConsoleFullAccessFromVercel
- ConsoleViewOnlyAccessFromVercel
- CostOptimizationHubAdminAccess
- CostOptimizationHubReadOnlyAccess
- CostOptimizationHubServiceRolePolicy
- CustomerProfilesServiceLinkedRolePolicy
- DatabaseAdministrator
- DataScientist
- DAXServiceRolePolicy
- DBModDiscoveryAndAssessment
- DBModProvisioningAndMigration
- DBModVirtualSource
- DeclarativePoliciesEC2Report
- DynamoDBCloudWatchContributorInsightsServiceRolePolicy
- DynamoDBGlobalTableSettingsManagementServiceRolePolicy
- DynamoDBKinesisReplicationServiceRolePolicy
- DynamoDBReplicationServiceRolePolicy
- EC2ApplicationStatusChecksServiceRolePolicy
- EC2FastLaunchFullAccess
- EC2FastLaunchServiceRolePolicy
- EC2FleetTimeShiftableServiceRolePolicy
- Ec2ImageBuilderCrossAccountDistributionAccess
- EC2ImageBuilderExecutionPolicy
- EC2ImageBuilderLifecycleExecutionPolicy
- EC2InstanceConnect
- Ec2InstanceConnectEndpoint
- EC2InstanceProfileForImageBuilder
- EC2InstanceProfileForImageBuilderECRContainerBuilds
- ECRReplicationServiceRolePolicy

- ECRTemplateServiceRolePolicy
- ElastiCacheServiceRolePolicy
- ElasticLoadBalancingFullAccess
- ElasticLoadBalancingReadOnly
- ElementalActivationsDownloadSoftwareAccess
- ElementalActivationsFullAccess
- ElementalActivationsGenerateLicenses
- ElementalActivationsReadOnlyAccess
- ElementalAppliancesSoftwareFullAccess
- ElementalAppliancesSoftwareReadOnlyAccess
- ElementalSupportCenterFullAccess
- EMRDescribeClusterPolicyForEMRWAL
- EndUserMessagingServiceRolePolicy
- FinOpsAgentAgentPolicy
- FinOpsAgentOperatorPolicy
- FMSServiceRolePolicy
- FSxDeleteServiceLinkedRoleAccess
- GameLiftContainerFleetPolicy
- GameLiftGameServerGroupPolicy
- GitLabDuoWithAmazonQPermissionsPolicy
- GlobalAcceleratorFullAccess
- GlobalAcceleratorReadOnlyAccess
- GreengrassOTAUpdateArtifactAccess
- GroundTruthSyntheticConsoleFullAccess
- GroundTruthSyntheticConsoleReadOnlyAccess
- Health_OrganizationsServiceRolePolicy
- IAMAccessAdvisorReadOnly
- IAMAccessAnalyzerFullAccess
- IAMAccessAnalyzerReadOnlyAccess
- IAMFullAccess

- IAMReadOnlyAccess
- IAMSelfManageServiceSpecificCredentials
- IAMUserChangePassword
- IAMUserSSHKeys
- IVSFullAccess
- IVSReadOnlyAccess
- IVSRecordToS3
- KafkaConnectServiceRolePolicy
- KafkaServiceRolePolicy
- KeyspacesCDCServiceRolePolicy
- KeyspacesReplicationServiceRolePolicy
- LakeFormationDataAccessServiceRolePolicy
- LexBotPolicy
- LexChannelPolicy
- LightsailExportAccess
- MediaConnectGatewayInstanceRolePolicy
- MediaPackageServiceRolePolicy
- MemoryDBServiceRolePolicy
- MigrationHubDMSAccessServiceRolePolicy
- MigrationHubServiceRolePolicy
- MigrationHubSMSAccessServiceRolePolicy
- MonitronServiceRolePolicy
- MultiPartyApprovalFullAccess
- MultiPartyApprovalReadOnlyAccess
- NeptuneConsoleFullAccess
- NeptuneFullAccess
- NeptuneGraphReadOnlyAccess
- NeptuneReadOnlyAccess
- NetworkAdministrator
- NetworkSecurityDirectorServiceLinkedRolePolicy

- NetworkSecurityManagerServiceRolePolicy
- NovaActServiceRolePolicy
- OAMFullAccess
- OAMReadOnlyAccess
- OpensearchIngestionSelfManagedVpcePolicy
- PartnerCentralAccountManagementUserRoleAssociation
- PartnerCentralIncentiveBenefitManagement
- PowerUserAccess
- PricingPlanManagerFullAccess
- PricingPlanManagerReadonlyAccess
- QAppsServiceRolePolicy
- QBusinessQuicksightPluginPolicy
- QBusinessServiceRolePolicy
- QuickSightAccessForS3StorageManagementAnalyticsReadOnly
- RDSCloudHsmAuthorizationRole
- ReadOnlyAccess
- ReInventTicketApprovalAccess
- ResourceGroupsandTagEditorFullAccess
- ResourceGroupsandTagEditorReadOnlyAccess
- ResourceGroupsServiceRolePolicy
- ResourceGroupsTaggingAPITagUntagSupportedResources
- ROSAAmazonEBSCSIDriverOperatorPolicy
- ROSACloudNetworkConfigOperatorPolicy
- ROSAControlPlaneOperatorPolicy
- ROSAImageRegistryOperatorPolicy
- ROSAIngressOperatorPolicy
- ROSAInstallerPolicy
- ROSAKarpenterControllerPolicy
- ROSAKMSProviderPolicy
- ROSAKubeControllerPolicy

- ROSAManageSubscription
- ROSANodePoolManagementPolicy
- ROSASharedVPCEndpointPolicy
- ROSASharedVPCRoute53Policy
- ROSASRESupportPolicy
- ROSAWorkerInstancePolicy
- Route53RecoveryReadinessServiceRolePolicy
- Route53ResolverServiceRolePolicy
- RTBFabricServiceRolePolicy
- S3StorageLensServiceRolePolicy
- SageMakerStudioAdminIAMConsolePolicy
- SageMakerStudioAdminIAMDefaultExecutionPolicy
- SageMakerStudioAdminIAMPermissiveExecutionPolicy
- SageMakerStudioAdminProjectUserRolePolicy
- SageMakerStudioBedrockAgentServiceRolePolicy
- SageMakerStudioBedrockChatAgentUserRolePolicy
- SageMakerStudioBedrockEvaluationJobServiceRolePolicy
- SageMakerStudioBedrockFlowServiceRolePolicy
- SageMakerStudioBedrockFunctionExecutionRolePolicy
- SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy
- SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy
- SageMakerStudioBedrockPromptUserRolePolicy
- SageMakerStudioDomainExecutionRolePolicy
- SageMakerStudioDomainServiceRolePolicy
- SageMakerStudioEMRContainersSystemNamespaceRolePolicy
- SageMakerStudioEMRInstanceRolePolicy
- SageMakerStudioEMRServiceRolePolicy
- SageMakerStudioFullAccess
- SageMakerStudioProjectProvisioningRolePolicy
- SageMakerStudioProjectRoleMachineLearningPolicy

- SageMakerStudioProjectUserRolePermissionsBoundary
- SageMakerStudioProjectUserRolePolicy
- SageMakerStudioQueryExecutionRolePolicy
- SageMakerStudioUserIAMConsolePolicy
- SageMakerStudioUserIAMDefaultExecutionPolicy
- SageMakerStudioUserIAMPermissiveExecutionPolicy
- SecretsManagerReadWrite
- SecurityAgentWebAppAPIPolicy
- SecurityAgentWebAppPolicy
- SecurityAudit
- SecurityLakeResourceManagementServiceRolePolicy
- SecurityLakeServiceLinkedRole
- ServerMigration_ServiceRole
- ServerMigrationConnector
- ServerMigrationServiceConsoleFullAccess
- ServerMigrationServiceLaunchRole
- ServerMigrationServiceRoleForInstanceValidation
- ServiceQuotasFullAccess
- ServiceQuotasReadOnlyAccess
- ServiceQuotasServiceRolePolicy
- SignInLocalDevelopmentAccess
- SimpleWorkflowFullAccess
- SMSVoiceServiceRolePolicy
- SplitCostAllocationDataServiceRolePolicy
- SSMQuickSetupRolePolicy
- SupportUser
- SystemAdministrator
- TranslateFullAccess
- TranslateReadOnly
- ViewOnlyAccess

- VMImportExportRoleForAWSConnector
- VPCLatticeFullAccess
- VPCLatticeReadOnlyAccess
- VPCLatticeServicesInvokeAccess
- WAFLoggingServiceRolePolicy
- WAFRegionalLoggingServiceRolePolicy
- WAFV2LoggingServiceRolePolicy
- WellArchitectedAgentResourceScanning
- WellArchitectedConsoleFullAccess
- WellArchitectedConsoleReadOnlyAccess
- WorkLinkServiceRolePolicy

AccessAnalyzerServiceRolePolicy

Deskripsi: Izinkan Access Analyzer menganalisis metadata sumber daya

`AccessAnalyzerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 02 Desember 2019, 17:13 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v23 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessAnalyzerServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ecr:DescribeRepositories",
        "ecr:GetAccountSetting",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "iam:GetRole",
        "iam:ListEntitiesForPolicy",
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListRoleTags",
        "iam:ListUserTags",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetUser",
        "iam:GetGroup",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:GetServiceLastAccessedDetails",
        "iam:ListAccessKeys",
        "iam:GetLoginProfile",
        "iam:GetAccessKeyLastUsed",
```

```
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListUserPolicies",
        "iam:GetUserPolicy",
        "iam:ListAttachedUserPolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListGroupsForUser",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:ListGrants",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListVersionsByFunction",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "s3:DescribeMultiRegionAccessPointOperation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
```

```
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
        "s3express:GetBucketPolicy",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:ListAccessPointsForDirectoryBuckets",
        "sns:GetTopicAttributes",
        "sns:ListTopics",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AccountAccessManagerServiceRolePolicy

Deskripsi: Memberikan izin pengelola akses akun untuk mengelola Akun AWS akses

`AccountAccessManagerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 29 Juni 2026, 19:12 UTC
- Waktu teredit: 29 Juni 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccountAccessManagerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "organizations:DescribeAccount",
      "Resource" : "arn:aws:organizations::*:account/o-*/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AccountManagementFromVercel

Deskripsi: Untuk digunakan dengan akun yang dibuat melalui integrasi Vercel Marketplace dengan AWS. Menyediakan akses ke manajemen akun, pemberitahuan, analisis biaya dan penggunaan, dan manajemen penyedia identitas.

`AccountManagementFromVercel`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AccountManagementFromVercel` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Desember 2025, 16:34 UTC
- Waktu yang diedit: 07 Mei 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AccountManagementFromVercel`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:CloseAccount",
        "bcm-recommended-actions:ListRecommendedActions",
        "ce:GetCostAndUsage",
        "cur:GetUsageReport",
        "iam:ListSAMLProviders",
        "freetier:GetFreeTierUsage",
        "freetier:GetAccountPlanState"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:UpdateSamlProvider",
        "iam:GetSamlProvider"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VercelInstallId" : "${aws:PrincipalTag/VercelInstallId}"
        }
      }
    },
    {
      "Sid" : "ManageServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:DeleteRole"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/Vercel/Service_2026_04_16",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VercelInstallId" : "${aws:PrincipalTag/VercelInstallId}",
          "iam:PermissionsBoundary" : [
            "arn:aws:iam::partner:policy/permissions-boundary/vercel.com/
VercelMarketplaceServiceRoleBoundary_2026_04_16"
          ]
        }
      }
    },
    {
      "Sid" : "TagManageServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Vercel/Service_2026_04_16",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/VercelInstallId" : "${aws:PrincipalTag/VercelInstallId}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AdministratorAccess

Deskripsi: Menyediakan akses penuh ke AWS layanan dan sumber daya.

`AdministratorAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AdministratorAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu teredit: 06 Februari 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AdministratorAccess-Amplify

Deskripsi: Memberikan izin administratif akun sambil secara eksplisit mengizinkan akses langsung ke sumber daya yang dibutuhkan oleh aplikasi Amplify.

`AdministratorAccess-Amplify`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AdministratorAccess-Amplify` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2020, 19:03 UTC
- Waktu teredit: 04 April 2024, 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-Amplify`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CLICloudformationPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
```

```
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplate",
        "cloudformation:UpdateStack",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:DeleteStackSet",
        "cloudformation:DescribeStackSet",
        "cloudformation:UpdateStackSet",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/amplify-*"
      ]
    },
    {
      "Sid" : "CLIManageviaCFNPolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoleTags",
        "iam:TagRole",
        "iam:AttachRolePolicy",
        "iam:CreatePolicy",
        "iam:DeletePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePolicy",
        "iam:UntagRole",
        "iam:UpdateRole",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetRolePolicy",
        "iam:PassRole",
        "iam:ListPolicyVersions",
        "iam:CreatePolicyVersion",
        "iam:DeletePolicyVersion",
        "iam:CreateRole",
        "iam:ListRolePolicies",
        "iam:PutRolePermissionsBoundary",
        "iam:DeleteRolePermissionsBoundary",
```

```
        "appsync:CreateApiKey",
        "appsync:CreateDataSource",
        "appsync:CreateFunction",
        "appsync:CreateResolver",
        "appsync:CreateType",
        "appsync:DeleteApiKey",
        "appsync:DeleteDataSource",
        "appsync:DeleteFunction",
        "appsync:DeleteResolver",
        "appsync:DeleteType",
        "appsync:GetDataSource",
        "appsync:GetFunction",
        "appsync:GetIntrospectionSchema",
        "appsync:GetResolver",
        "appsync:GetSchemaCreationStatus",
        "appsync:GetType",
        "appsync:GraphQL",
        "appsync:ListApiKeys",
        "appsync:ListDataSources",
        "appsync:ListFunctions",
        "appsync:ListGraphqlApis",
        "appsync:ListResolvers",
        "appsync:ListResolversByFunction",
        "appsync:ListTypes",
        "appsync:StartSchemaCreation",
        "appsync:UntagResource",
        "appsync:UpdateApiKey",
        "appsync:UpdateDataSource",
        "appsync:UpdateFunction",
        "appsync:UpdateResolver",
        "appsync:UpdateType",
        "appsync:TagResource",
        "appsync:CreateGraphqlApi",
        "appsync:DeleteGraphqlApi",
        "appsync:GetGraphqlApi",
        "appsync:ListTagsForResource",
        "appsync:UpdateGraphqlApi",
        "apigateway:DELETE",
        "apigateway:GET",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT",
        "cognito-idp:CreateUserPool",
        "cognito-identity:CreateIdentityPool",
```

```
        "cognito-identity:DeleteIdentityPool",
        "cognito-identity:DescribeIdentity",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:SetIdentityPoolRoles",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:UpdateIdentityPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteUserPool",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:UpdateUserPoolClient",
        "cognito-idp:CreateGroup",
        "cognito-idp:DeleteGroup",
        "cognito-identity:TagResource",
        "cognito-idp:TagResource",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:SetUserPoolMfaConfig",
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeAsync",
        "lambda:InvokeFunction",
        "lambda:RemovePermission",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:AddLayerVersionPermission",
        "lambda:CreateEventSourceMapping",
        "lambda:DeleteEventSourceMapping",
        "lambda:DeleteLayerVersion",
        "lambda:GetEventSourceMapping",
        "lambda:GetLayerVersion",
        "lambda:ListEventSourceMappings",
        "lambda:ListLayerVersions",
        "lambda:PublishLayerVersion",
        "lambda:RemoveLayerVersionPermission",
        "lambda:UpdateEventSourceMapping",
```

```
        "dynamodb:CreateTable",
        "dynamodb:DeleteItem",
        "dynamodb:DeleteTable",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListStreams",
        "dynamodb:PutItem",
        "dynamodb:TagResource",
        "dynamodb:ListTagsOfResource",
        "dynamodb:UntagResource",
        "dynamodb:UpdateContinuousBackups",
        "dynamodb:UpdateItem",
        "dynamodb:UpdateTable",
        "dynamodb:UpdateTimeToLive",
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:PutBucketAcl",
        "s3:PutBucketCORS",
        "s3:PutBucketNotification",
        "s3:PutBucketPolicy",
        "s3:PutBucketWebsite",
        "s3:PutObjectAcl",
        "cloudfront:CreateCloudFrontOriginAccessIdentity",
        "cloudfront:CreateDistribution",
        "cloudfront:DeleteCloudFrontOriginAccessIdentity",
        "cloudfront:DeleteDistribution",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetCloudFrontOriginAccessIdentityConfig",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:TagResource",
        "cloudfront:UntagResource",
        "cloudfront:UpdateCloudFrontOriginAccessIdentity",
        "cloudfront:UpdateDistribution",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "mobiletargeting:GetApp",
        "kinesis:AddTagsToStream",
        "kinesis:CreateStream",
```

```
        "kinesis:DeleteStream",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListTagsForStream",
        "kinesis:PutRecords",
        "es:AddTags",
        "es:CreateElasticsearchDomain",
        "es:DeleteElasticsearchDomain",
        "es:DescribeElasticsearchDomain",
        "es:UpdateElasticsearchDomainConfig",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CLISDKCalls",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetIntrospectionSchema",
        "appsync:GraphQL",
        "appsync:UpdateApiKey",
        "appsync:ListApiKeys",
        "amplify:*",
        "amplifybackend:*",
        "amplifyuibuilder:*",
        "sts:AssumeRole",
        "mobiletargeting:*",
        "cognito-idp:AdminAddUserToGroup",
        "cognito-idp:AdminCreateUser",
        "cognito-idp:CreateGroup",
        "cognito-idp:DeleteGroup",
        "cognito-idp:DeleteUser",
        "cognito-idp:ListUsers",
        "cognito-idp:AdminGetUser",
        "cognito-idp:ListUsersInGroup",
        "cognito-idp:AdminDisableUser",
```

```
        "cognito-idp:AdminRemoveUserFromGroup",
        "cognito-idp:AdminResetUserPassword",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:ListGroups",
        "cognito-idp:AdminListUserAuthEvents",
        "cognito-idp:AdminDeleteUser",
        "cognito-idp:AdminConfirmSignUp",
        "cognito-idp:AdminEnableUser",
        "cognito-idp:AdminUpdateUserAttributes",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DeleteUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:CreateUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:AdminSetUserPassword",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:SetIdentityPoolRoles",
        "cognito-identity:CreateIdentityPool",
        "cognito-identity:DeleteIdentityPool",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:DescribeIdentityPool",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "lambda:GetFunction",
        "lambda:CreateFunction",
        "lambda:AddPermission",
        "lambda:DeleteFunction",
        "lambda:DeleteLayerVersion",
        "lambda:InvokeFunction",
        "lambda:ListLayerVersions",
        "iam:PutRolePolicy",
        "iam:CreatePolicy",
        "iam:AttachRolePolicy",
        "iam:ListPolicyVersions",
        "iam:ListAttachedRolePolicies",
        "iam:CreateRole",
        "iam:PassRole",
        "iam:ListRolePolicies",
```

```
        "iam:DeleteRolePolicy",
        "iam:CreatePolicyVersion",
        "iam:DeletePolicyVersion",
        "iam:DeleteRole",
        "iam:DetachRolePolicy",
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks",
        "sns:CreateSMSSandboxPhoneNumber",
        "sns:GetSMSSandboxAccountStatus",
        "sns:VerifySMSSandboxPhoneNumber",
        "sns:DeleteSMSSandboxPhoneNumber",
        "sns:ListSMSSandboxPhoneNumbers",
        "sns:ListOriginationNumbers",
        "rekognition:DescribeCollection",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "lex:GetBot",
        "lex:GetBuiltinIntent",
        "lex:GetBuiltinIntents",
        "lex:GetBuiltinSlotTypes",
        "cloudformation:GetTemplateSummary",
        "codecommit:GitPull",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetCloudFrontOriginAccessIdentityConfig",
        "polly:DescribeVoices"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifySSMCalls",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:GetParametersByPath",
        "ssm:GetParameters",
        "ssm:GetParameter",
        "ssm:DeleteParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/amplify/*"
    },
    {
      "Sid" : "GeoPowerUser",
      "Effect" : "Allow",
```

```
      "Action" : [
        "geo:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifyEcrSDKCalls",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifyStorageSDKCalls",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteBucketWebsite",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutBucketAcl",
        "s3:PutBucketCORS",
        "s3:PutBucketNotification",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutBucketWebsite",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifySSRCalls",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudfront:CreateCloudFrontOriginAccessIdentity",
        "cloudfront:CreateDistribution",
        "cloudfront:CreateInvalidation",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListCloudFrontOriginAccessIdentities",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByLambdaFunction",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:ListFieldLevelEncryptionConfigs",
        "cloudfront:ListFieldLevelEncryptionProfiles",
        "cloudfront:ListInvalidations",
        "cloudfront:ListPublicKeys",
        "cloudfront:ListStreamingDistributions",
        "cloudfront:UpdateDistribution",
        "cloudfront:TagResource",
        "cloudfront:UntagResource",
        "cloudfront:ListTagsForResource",
        "cloudfront:DeleteDistribution",
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:CreateServiceLinkedRole",
        "iam:GetRole",
        "iam:PutRolePolicy",
        "iam:PassRole",
        "lambda:CreateFunction",
        "lambda:EnableReplication",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:PublishVersion",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource",
        "route53:ChangeResourceRecordSets",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "s3:CreateBucket",
        "s3:GetAccelerateConfiguration",
        "s3:GetObject",
        "s3:ListBucket",
```

```
        "s3:PutAccelerateConfiguration",
        "s3:PutBucketPolicy",
        "s3:PutObject",
        "s3:PutBucketTagging",
        "s3:GetBucketTagging",
        "lambda:ListEventSourceMappings",
        "lambda:CreateEventSourceMapping",
        "iam:UpdateAssumeRolePolicy",
        "iam:DeleteRolePolicy",
        "sqs:CreateQueue",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:SetQueueAttributes",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:UpdateApp",
        "amplify:UpdateBranch"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifySSRViewLogGroups",
      "Effect" : "Allow",
      "Action" : "logs:DescribeLogGroups",
      "Resource" : "arn:aws:logs:*:*:log-group:*"
    },
    {
      "Sid" : "AmplifySSRCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/amplify/*"
    },
    {
      "Sid" : "AmplifySSRPushLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/amplify/*:log-stream:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AdministratorAccess-AWSElasticBeanstalk

Deskripsi: Memberikan izin administratif akun. Secara eksplisit memungkinkan pengembang dan administrator untuk mendapatkan akses langsung ke sumber daya yang mereka butuhkan untuk mengelola aplikasi AWS Elastic Beanstalk

`AdministratorAccess-AWSElasticBeanstalk`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AdministratorAccess-AWSElasticBeanstalk` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 Januari 2021, 19:36 UTC
- Waktu teredit: 19 Mei 2026, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:Describe*",
        "acm:List*",
        "autoscaling:Describe*",
        "cloudformation:Describe*",
        "cloudformation:Estimate*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:Validate*",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "codecommit:Get*",
        "codecommit:UploadArchive",
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroup*",
        "ec2:CreateLaunchTemplate*",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DeleteLaunchTemplate*",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroup*",
        "ecs:CreateCluster",
        "ecs:DeRegisterTaskDefinition",
        "ecs:Describe*",
        "ecs:List*",
        "ecs:RegisterTaskDefinition",
        "elasticbeanstalk:*",
        "elasticloadbalancing:Describe*",
        "iam:GetRole",
```

```
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListServerCertificates",
        "logs:Describe*",
        "rds:Describe*",
        "s3:ListAllMyBuckets",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:*"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CancelUpdateStack",
        "cloudformation:ContinueUpdateRollback",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:SignalResource",
        "cloudformation:TagResource",
        "cloudformation:UntagResource",
        "cloudformation:UpdateStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:awseb-*",
        "arn:aws:cloudwatch:*:*:alarm:eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:StartBuild"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/Elastic-Beanstalk-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable",
        "dynamodb:TagResource"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/awseb-e-*",
        "arn:aws:dynamodb:*:*:table/eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
```

```
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteCluster"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/awseb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:*Rule",
        "elasticloadbalancing:*Tags",
        "elasticloadbalancing:SetRulePriorities",
        "elasticloadbalancing:SetSecurityGroups"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:*"
      ],
```

```
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/eb-*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/eb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/*/awseb-*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/*/eb-*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/awseb-*/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/eb-*/*/*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-elasticbeanstalk*",
        "arn:aws:iam::*:instance-profile/aws-elasticbeanstalk*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-elasticbeanstalk*",
      "Condition" : {
        "ArnLike" : {
          "iam:PolicyArn" : [
            "arn:aws:iam::aws:policy/AWSElasticBeanstalk*",
            "arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalk*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/autoscaling.amazonaws.com/
AWSServiceRoleForAutoScaling",
        "arn:aws:iam::*:role/aws-service-role/elasticbeanstalk.amazonaws.com/
AWSServiceRoleForElasticBeanstalk",
        "arn:aws:iam::*:role/aws-service-role/elasticloadbalancing.amazonaws.com/
AWSServiceRoleForElasticLoadBalancing",
        "arn:aws:iam::*:role/aws-service-role/
managedupdates.elasticbeanstalk.amazonaws.com/AWSServiceRoleForElasticBeanstalk",
        "arn:aws:iam::*:role/aws-service-role/
maintenance.elasticbeanstalk.amazonaws.com/AWSServiceRoleForElasticBeanstalk"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "elasticbeanstalk.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "managedupdates.elasticbeanstalk.amazonaws.com",
            "maintenance.elasticbeanstalk.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:*DBSubnetGroup",
        "rds:AuthorizeDBSecurityGroupIngress",
        "rds:CreateDBInstance",
        "rds:CreateDBSecurityGroup",
        "rds:DeleteDBInstance",
        "rds:DeleteDBSecurityGroup",
        "rds:ModifyDBInstance",
        "rds:RestoreDBInstanceFromDBSnapshot"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:secgrp:awseb-e-*",
        "arn:aws:rds:*:*:secgrp:eb-*",
        "arn:aws:rds:*:*:snapshot:*",
        "arn:aws:rds:*:*:subgrp:awseb-e-*",
        "arn:aws:rds:*:*:subgrp:eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Delete*",
        "s3:Get*",
        "s3:Put*"
```

```
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucket*",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketOwnershipControls"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:GetTopicAttributes",
        "sns:Publish",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:*QueueAttributes",
        "sqs:CreateQueue",
        "sqs:DeleteQueue",
        "sqs:SendMessage",
        "sqs:TagQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:awseb-e-*",
        "arn:aws:sqs:*:*:eb-*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AgentRegistryFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Agen Registry

`AgentRegistryFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AgentRegistryFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Agustus 2026, 18:12 UTC
- Waktu teredit: 31 Agustus 2026, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AgentRegistryFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AgentRegistryFullAccess",
      "Effect" : "Allow",
      "Action" : "agent-registry:*",
      "Resource" : "arn:aws:agent-registry:*:*:*"
    },
    {
      "Sid" : "AgentRegistryPassRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "agent-registry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AgentRegistryWorkloadIdentityAccess",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:CreateWorkloadIdentity",
        "bedrock-agentcore:DeleteWorkloadIdentity",
        "bedrock-agentcore:GetWorkloadAccessToken",
        "bedrock-agentcore:GetWorkloadIdentity"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:workload-identity-directory/*"
    },
    {
      "Sid" : "AllowGetResourceOauth2TokenForOauthBasedSynchronization",
```

```
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GetResourceOauth2Token"
      ],
      "Resource" : [
        "arn:aws:bedrock-agentcore:*:*:credential-provider/*",
        "arn:aws:bedrock-agentcore:*:*:workload-identity-directory/*",
        "arn:aws:bedrock-agentcore:*:*:token-vault/*/oauth2credentialprovider/*"
      ]
    },
    {
      "Sid" : "AllowListOauth2CredentialsProvidersForConsolePicker",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:ListOauth2CredentialProviders"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:*"
    },
    {
      "Sid" : "IAMListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "AgentRegistryKMSDecryptKeyForSynchronization",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AgentRegistryKMSDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
```

```
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "agent-registry.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AgentRegistryKMSCryptoOps",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "agent-registry.*.amazonaws.com",
          "kms:EncryptionContext:aws:agent-registry:registry-arn" : "arn:aws:agent-
registry:*:*:registry/*"
        }
      }
    },
    {
      "Sid" : "AgentRegistryKMSCreateGrant",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "agent-registry.*.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
```

```
            "ReEncryptTo",
            "DescribeKey",
            "CreateGrant"
          ]
        },
        "Null" : {
          "kms:GrantOperations" : "false"
        }
      }
    },
    {
      "Sid" : "AgentRegistrySecretsManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*"
    },
    {
      "Sid" : "AgentRegistryServiceLinkedRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/agent-registry.amazonaws.com/
AWSServiceRoleForAgentRegistry",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "agent-registry.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AgentRegistryReadOnlyAccess

Deskripsi: Kebijakan untuk ReadOnly akses ke AWS Agen Registry

`AgentRegistryReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AgentRegistryReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Agustus 2026, 18:12 UTC
- Waktu teredit: 06 Agustus 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/AgentRegistryReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AgentRegistryReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "agent-registry:GetRegistry",
        "agent-registry:ListRegistries",
        "agent-registry:GetRegistryRecord",
        "agent-registry:ListRegistryRecords",
        "agent-registry:ListDiscoverableRegistryRecords",
        "agent-registry:GetDiscoverableRegistryRecord",
```

```
        "agent-registry:InvokeRegistryMcp",
        "agent-registry:SearchDiscoverableRegistryRecords",
        "agent-registry:ListTagsForResource"
      ],
      "Resource" : "arn:aws:agent-registry:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AIDevOpsAgentAccessPolicy

Deskripsi: Memberikan izin yang diperlukan oleh AWS DevOps Agen untuk melakukan penyelidikan dan melakukan analisis pada AWS sumber daya pelanggan.

`AIDevOpsAgentAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AIDevOpsAgentAccessPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Maret 2026, 03:42 UTC
- Waktu teredit: 24 September 2026, 20:57 UTC
- ARN: `arn:aws:iam::aws:policy/AIDevOpsAgentAccessPolicy`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOPSServiceWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:StartQuery",
        "support:CreateCase"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AIOPSServiceAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:List*",
        "acm-pca:Describe*",
        "acm-pca:GetCertificate",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:List*",
        "acm:DescribeCertificate",
        "acm:GetAccountConfiguration",
        "acm:GetCertificate",
        "acm:ListCertificates",
        "aidevops:GetAsset",
        "aidevops:GetAssetContent",
        "aidevops:GetAssetFile",
        "aidevops:GetKnowledgeItem",
        "aidevops:ListAssetFiles",
        "aidevops:ListAssets",
        "aidevops:ListAssetTypes",
        "aidevops:ListAssetVersions",
        "aidevops:ListKnowledgeItems",
        "airflow:GetEnvironment",
```

```
        "airflow:List*",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:List*",
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:List*",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetEnvironment",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:List*",
        "appflow:Describe*",
        "appflow:List*",
        "application-autoscaling:Describe*",
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:List*",
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "apprunner:Describe*",
        "apprunner:List*",
        "appstream:Describe*",
        "appstream:List*",
        "appsync:GetApiAssociation",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
        "appsync:GetFunction",
        "appsync:GetGraphqlApi",
        "appsync:GetGraphqlApiEnvironmentVariables",
        "appsync:GetIntrospectionSchema",
        "appsync:GetResolver",
        "appsync:GetSourceApiAssociation",
        "appsync:List*",
        "aps:Describe*",
        "aps:List*",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:List*",
```

```
        "athena:GetCapacityAssignmentConfiguration",
        "athena:GetCapacityReservation",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:List*",
        "auditmanager:GetAssessment",
        "auditmanager:List*",
        "autoscaling:Describe*",
        "backup-gateway:GetHypervisor",
        "backup-gateway:List*",
        "backup:Describe*",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:List*",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:List*",
        "bcm-data-exports:Get*",
        "bcm-data-exports:List*",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetCustomModel",
        "bedrock:GetDataSource",
        "bedrock:GetFoundationModel",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:List*",
        "budgets:Describe*",
        "budgets:List*",
        "budgets:ViewBudget",
        "ce:Describe*",
        "ce:Get*",
```

```
        "ce:List*",
        "chatbot:Describe*",
        "chatbot:GetMicrosoftTeamsChannelConfiguration",
        "chatbot:List*",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:List*",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:List*",
        "cloudformation:Describe*",
        "cloudformation:GetResource",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:List*",
        "cloudfront:Describe*",
        "cloudfront:GetCachePolicy",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetContinuousDeploymentPolicy",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetFunction",
        "cloudfront:GetKeyGroup",
        "cloudfront:GetMonitoringSubscription",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetOriginRequestPolicy",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:List*",
        "cloudtrail:Describe*",
        "cloudtrail:GetChannel",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetQueryResults",
        "cloudtrail:GetResourcePolicy",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:List*",
```

```
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetInsightRuleReport",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricStream",
        "cloudwatch:GetOTelEnrichment",
        "cloudwatch:GetService",
        "cloudwatch:GetServiceLevelObjective",
        "cloudwatch:List*",
        "codeartifact:Describe*",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:List*",
        "codebuild:BatchGetFleets",
        "codebuild:List*",
        "codecommit:BatchDescribe*",
        "codecommit:BatchGet*",
        "codecommit:Describe*",
        "codecommit:EvaluatePullRequestApprovalRules",
        "codecommit:GetApprovalRuleTemplate",
        "codecommit:GetBranch",
        "codecommit:GetComment",
        "codecommit:GetCommentReactions",
        "codecommit:GetCommentsForComparedCommit",
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommit",
        "codecommit:GetCommitHistory",
        "codecommit:GetCommitsFromMergeBase",
        "codecommit:GetDifferences",
        "codecommit:GetMergeCommit",
        "codecommit:GetMergeConflicts",
        "codecommit:GetMergeOptions",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetPullRequest",
        "codecommit:GetPullRequestApprovalStates",
        "codecommit:GetPullRequestOverrideState",
        "codecommit:GetReferences",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:GetTree",
        "codecommit:GetUploadArchiveStatus",
```

```
        "codecommit:List*",
        "codedeploy:BatchGetDeployments",
        "codedeploy:BatchGetDeploymentTargets",
        "codedeploy:GetApplication",
        "codedeploy:GetDeploymentConfig",
        "codedeploy:GetDeploymentTarget",
        "codedeploy:List*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:List*",
        "codeguru-reviewer:Describe*",
        "codeguru-reviewer:List*",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:List*",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:GetSyncConfiguration",
        "codestar-connections:List*",
        "codestar-notifications:Describe*",
        "codestar-notifications:List*",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeRiskConfiguration",
        "cognito-idp:DescribeUserImportJob",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetLogDeliveryConfiguration",
        "cognito-idp:GetUICustomization",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:GetWebACLForResource",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListTagsForResource",
```

```
        "comprehend:Describe*",
        "comprehend:List*",
        "config:Describe*",
        "config:GetAggregateResourceConfig",
        "config:GetStoredQuery",
        "config:List*",
        "config:SelectAggregateResourceConfig",
        "connect:Describe*",
        "connect:GetMetricDataV2",
        "connect:GetTaskTemplate",
        "connect:List*",
        "cur:Describe*",
        "cur:Get*",
        "databrew:Describe*",
        "databrew:List*",
        "datapipeline:Describe*",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:List*",
        "datasync:Describe*",
        "datasync:List*",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetLicenseEndpoint",
        "deadline:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetStorageProfile",
        "deadline:List*",
        "detective:GetMembers",
        "detective:List*",
        "devicefarm:GetDevicePool",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:GetVPCEConfiguration",
        "devicefarm:List*",
        "devops-guru:Describe*",
        "devops-guru:GetResourceCollection",
        "devops-guru:List*",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
```

```
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeHostedConnections",
        "directconnect:DescribeInterconnects",
        "directconnect:DescribeLags",
        "directconnect:DescribeTags",
        "directconnect:DescribeVirtualInterfaces",
        "dms:Describe*",
        "dms:List*",
        "ds:Describe*",
        "dynamodb:Describe*",
        "dynamodb:GetResourcePolicy",
        "dynamodb:List*",
        "ec2:Describe*",
        "ec2:GetAssociatedEnclaveCertificateIamRoles",
        "ec2:GetCapacityManagerAttributes",
        "ec2:GetCapacityManagerMetricData",
        "ec2:GetCapacityManagerMonitoredTagKeys",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayRoutes",
        "ecr:Describe*",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:List*",
        "ecs:Describe*",
        "ecs:List*",
        "eks:AccessKubernetesApi",
        "eks:Describe*",
        "eks:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
```

```
        "elasticfilesystem:Describe*",
        "elasticloadbalancing:GetResourcePolicy",
        "elasticloadbalancing:GetTrustStoreCaCertificatesBundle",
        "elasticloadbalancing:GetTrustStoreRevocationContent",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "emr-containers:Describe*",
        "emr-containers:List*",
        "emr-serverless:GetApplication",
        "emr-serverless:List*",
        "es:Describe*",
        "es:List*",
        "events:Describe*",
        "events:List*",
        "evidently:GetExperiment",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:List*",
        "firehose:Describe*",
        "firehose:List*",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:List*",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:List*",
        "forecast:Describe*",
        "forecast:List*",
        "frauddetector:BatchGetVariable",
        "frauddetector:Describe*",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModelVersion",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
```

```
        "frauddetector:GetVariables",
        "frauddetector:List*",
        "fsx:Describe*",
        "gamelift:Describe*",
        "gamelift:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:BatchGetJobs",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlerMetrics",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDataQualityResult",
        "glue:GetJob",
        "glue:GetJobBookmark",
        "glue:GetJobRun",
        "glue:GetJobRuns",
        "glue:getPartition",
        "glue:GetPartitions",
        "glue:GetRegistry",
        "glue:GetResourcePolicy",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetWorkflow",
        "glue:GetWorkflowRun",
        "glue:List*",
        "glue:querySchemaVersionMetadata",
        "grafana:Describe*",
        "grafana:List*",
        "greengrass:Describe*",
        "greengrass:GetDeployment",
        "greengrass:List*",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
```

```
        "groundstation:GetMissionProfile",
        "groundstation:List*",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:GetIPSet",
        "guardduty:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:List*",
        "health:Describe*",
        "healthlake:Describe*",
        "healthlake:List*",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetLoginProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccountAliases",
        "iam:ListAttachedRolePolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListOpenIDConnectProviders",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListServerCertificates",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroups",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
```

```
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:GetWorkflow",
        "imagebuilder:List*",
        "inspector2:List*",
        "inspector2:SearchVulnerabilities",
        "inspector:Describe*",
        "inspector:List*",
        "internetmonitor:GetMonitor",
        "internetmonitor:List*",
        "iot:Describe*",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetPolicy",
        "iot:GetThingShadow",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:GetV2LoggingOptions",
        "iot:List*",
        "iotanalytics:Describe*",
        "iotanalytics:List*",
        "iotevents:Describe*",
        "iotevents:List*",
        "iotsitewise:Describe*",
        "iotsitewise:List*",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:List*",
        "ivs:GetChannel",
        "ivs:GetEncoderConfiguration",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:List*",
```

```
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:List*",
        "kafka:Describe*",
        "kafka:GetClusterPolicy",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kendra:Describe*",
        "kendra:List*",
        "kinesis:Describe*",
        "kinesis:GetResourcePolicy",
        "kinesis:List*",
        "kinesisanalytics:Describe*",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kms:DescribeCustomKeyStores",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:GetParametersForImport",
        "kms:GetPublicKey",
        "kms:ListAliases",
        "kms:ListGrants",
        "kms:ListKeyPolicies",
        "kms:ListKeyRotations",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "kms:ListRetirableGrants",
        "lakeformation:Describe*",
        "lakeformation:GetLFTag",
        "lakeformation:GetResourceLFTags",
        "lakeformation:List*",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
```

```
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:List*",
        "launchwizard:GetDeployment",
        "launchwizard:List*",
        "license-manager:GetLicense",
        "license-manager:List*",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:Describe*",
        "logs:FilterLogEvents",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopLiveTail",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:List*",
        "macie2:GetAllowList",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsFilter",
        "macie2:GetMacieSession",
```

```
        "macie2:List*",
        "mediaconnect:Describe*",
        "mediaconnect:List*",
        "medialive:Describe*",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:List*",
        "mediapackage-vod:Describe*",
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:List*",
        "memorydb:Describe*",
        "memorydb:List*",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:List*",
        "mq:Describe*",
        "mq:List*",
        "network-firewall:Describe*",
        "network-firewall:List*",
        "networkmanager:Describe*",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:List*",
```

```
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:List*",
        "omics:GetAnnotationStore",
        "omics:GetReferenceStore",
        "omics:GetRunGroup",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:List*",
        "organizations:Describe*",
        "organizations:List*",
        "osis:GetPipeline",
        "osis:List*",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:List*",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:List*",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:List*",
        "personalize:Describe*",
        "personalize:List*",
        "pi:Describe*",
        "pi:Get*",
        "pi:List*",
        "pipes:Describe*",
        "pipes:List*",
        "proton:GetEnvironmentTemplate",
        "proton:GetServiceTemplate",
        "proton:List*",
        "qbusiness:GetApplication",
        "qbusiness:GetDataSource",
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetRetriever",
        "qbusiness:GetWebExperience",
        "qbusiness:List*",
```

```
        "ram:GetPermission",
        "ram:GetResourceShares",
        "ram:List*",
        "rds:Describe*",
        "rds:List*",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
        "redshift:Describe*",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetRoute",
        "refactor-spaces:List*",
        "rekognition:Describe*",
        "rekognition:List*",
        "resiliencehub:Describe*",
        "resiliencehub:Get*",
        "resiliencehub:List*",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:List*",
        "resource-explorer-2:Search",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:List*",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:List*",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHealthCheckStatus",
        "route53:GetHostedZone",
        "route53:List*",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:List*",
```

```
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetOutpostResolver",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:List*",
        "rum:GetAppMonitor",
        "rum:List*",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListOutpostsWithS3",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointConfigurationForObjectLambda",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
```

```
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
        "s3:ListAllMyBuckets",
        "s3:ListTagsForResource",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:List*",
        "schemas:Describe*",
        "schemas:GetResourcePolicy",
        "schemas:List*",
        "secretsmanager:Describe*",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:List*",
        "securityhub:BatchGetAutomationRules",
        "securityhub:BatchGetSecurityControls",
        "securityhub:Describe*",
        "securityhub:GetConfigurationPolicy",
        "securityhub:GetConfigurationPolicyAssociation",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindingAggregator",
        "securityhub:GetFindings",
        "securityhub:GetInsights",
        "securityhub:List*",
        "securitylake:GetSubscriber",
        "securitylake:List*",
        "servicecatalog:Describe*",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:List*",
        "servicequotas:Get*",
        "servicequotas:List*",
        "ses:Describe*",
        "ses:GetAccount",
        "ses:GetAddonInstance",
        "ses:GetAddonSubscription",
        "ses:GetArchive",
        "ses:GetConfigurationSet",
```

```
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailIdentity",
        "ses:GetEmailTemplate",
        "ses:GetIngressPoint",
        "ses:GetRelay",
        "ses:GetRuleSet",
        "ses:GetTemplate",
        "ses:GetTrafficPolicy",
        "ses:List*",
        "shield:Describe*",
        "shield:List*",
        "signer:GetSigningProfile",
        "signer:List*",
        "sns:GetDataProtectionPolicy",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:List*",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:List*",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:List*",
        "ssm-sap:GetApplication",
        "ssm-sap:List*",
        "ssm:Describe*",
        "ssm:GetCommandInvocation",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetParameters",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:List*",
        "sso:DescribeAccountAssignmentCreationStatus",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetManagedApplicationInstance",
        "sso:GetPermissionsBoundaryForPermissionSet",
```

```
        "sso:GetSharedSsoConfiguration",
        "sso:ListAccountAssignments",
        "sso:ListApplicationAssignments",
        "sso:ListApplications",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListInstances",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:GetExecutionHistory",
        "states:Describe*",
        "states:List*",
        "support:DescribeCases",
        "synthetics:Describe*",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:List*",
        "tag:GetResources",
        "timestream:Describe*",
        "timestream:List*",
        "transfer:Describe*",
        "transfer:List*",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:List*",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetAuthPolicy",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:List*",
        "wafv2:GetIPSet",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRegexPatternSet",
        "wafv2:GetRuleGroup",
```

```
        "wafv2:GetSampledRequests",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:List*",
        "wisdom:Get*",
        "wisdom:List*",
        "wisdom:Query*",
        "wisdom:Retrieve",
        "wisdom:Search*",
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetUserSettings",
        "workspaces-web:List*",
        "workspaces:Describe*",
        "xray:BatchGetTraces",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:GetServiceGraph",
        "xray:GetTraceSummaries",
        "xray:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AIOPSAPIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integrations",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integrations/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
```

```
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*"
      ]
    },
    {
      "Sid" : "AllowListBucketAWSLogs",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "AWSLogs/*",
            "*/AWSLogs/*"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AIDevOpsAgentActionsPolicy

Deskripsi: Menyediakan izin yang ditingkatkan yang diperlukan oleh AWS DevOps Agen untuk melakukan mutasi yang disetujui operator atau tindakan yang ditingkatkan pada AWS sumber daya pelanggan selama peristiwa operasional.

`AIDevOpsAgentActionsPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AIDevOpsAgentActionsPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Juni 2026, 22:27 UTC
- Waktu teredit: 19 Agustus 2026, 22:47 UTC
- ARN: `arn:aws:iam::aws:policy/AIDevOpsAgentActionsPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIDevOpsElevatedAccess",
      "Effect" : "Allow",
      "NotAction" : [
        "account:*",
        "cognito-identity:*",
```

```
        "iam:*",
        "identitystore:*",
        "organizations:*",
        "ram:*",
        "rolesanywhere:*",
        "sso:*",
        "sts:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AIDevOpsElevatedCarveBacks",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetGovCloudAccountInformation",
        "account:GetPrimaryEmail",
        "account:ListRegions",
        "iam:ListRoles",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "sts:DecodeAuthorizationMessage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AIDevOpsAgentFullAccess

Deskripsi: Menyediakan akses penuh ke DevOps Agen Amazon melalui Konsol Manajemen AWS

`AIDevOpsAgentFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AIDevOpsAgentFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Maret 2026, 03:42 UTC
- Waktu teredit: 26 Juni 2026, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/AIDevOpsAgentFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIDevOpsAgentAccess",
      "Effect" : "Allow",
      "Action" : [
        "aidevops:AllowVendedLogDeliveryForResource",
        "aidevops:AssociateService",
        "aidevops:CreateAccessToken",
        "aidevops:CreateAgentSpace",
        "aidevops:CreateAsset",
        "aidevops:CreateAssetFile",
        "aidevops:CreateBacklogTask",
        "aidevops:CreateChat",
        "aidevops:CreateKnowledgeItem",
        "aidevops:CreateOneTimeLoginSession",
        "aidevops:CreatePrivateConnection",
        "aidevops:CreateTrigger",
```

```
        "aidevops:DeleteAgentSpace",
        "aidevops:DeleteAsset",
        "aidevops:DeleteAssetFile",
        "aidevops:DeleteKnowledgeItem",
        "aidevops:DeletePrivateConnection",
        "aidevops:DeleteTrigger",
        "aidevops:DeregisterService",
        "aidevops:DescribePrivateConnection",
        "aidevops:DescribeServices",
        "aidevops:DescribeSupportLevel",
        "aidevops:DisableOperatorApp",
        "aidevops:DisassociateService",
        "aidevops:DiscoverTopology",
        "aidevops:EnableOperatorApp",
        "aidevops:EndChatForCase",
        "aidevops:GetAccessToken",
        "aidevops:GetAccountUsage",
        "aidevops:GetAgentSpace",
        "aidevops:GetAsset",
        "aidevops:GetAssetContent",
        "aidevops:GetAssetFile",
        "aidevops:GetAssociation",
        "aidevops:GetBacklogTask",
        "aidevops:GetKnowledgeItem",
        "aidevops:GetOperatorApp",
        "aidevops:GetRecommendation",
        "aidevops:GetService",
        "aidevops:GetTrigger",
        "aidevops:InitiateChatForCase",
        "aidevops:ListAccessTokens",
        "aidevops:ListAgentSpaces",
        "aidevops:ListAssetFiles",
        "aidevops:ListAssets",
        "aidevops:ListAssetTypes",
        "aidevops:ListAssetVersions",
        "aidevops:ListAssociations",
        "aidevops:ListBacklogTasks",
        "aidevops:ListChats",
        "aidevops:ListExecutions",
        "aidevops:ListGoals",
        "aidevops:ListJournalRecords",
        "aidevops:ListKnowledgeItems",
        "aidevops:ListKnowledgeItemVersions",
        "aidevops:ListPendingMessages",
```

```
        "aidevops:ListPrivateConnections",
        "aidevops:ListRecommendations",
        "aidevops:ListServices",
        "aidevops:ListTagsForResource",
        "aidevops:ListTriggers",
        "aidevops:ListWebhooks",
        "aidevops:RegisterService",
        "aidevops:RevokeAccessToken",
        "aidevops:RotateAccessToken",
        "aidevops:SearchServiceAccessibleResource",
        "aidevops:SendMessage",
        "aidevops:TagResource",
        "aidevops:UntagResource",
        "aidevops:UpdateAgentSpace",
        "aidevops:UpdateApprovalAction",
        "aidevops:UpdateAsset",
        "aidevops:UpdateAssetFile",
        "aidevops:UpdateAssociation",
        "aidevops:UpdateBacklogTask",
        "aidevops:UpdateGoal",
        "aidevops:UpdateKnowledgeItem",
        "aidevops:UpdateOperatorAppIdpConfig",
        "aidevops:UpdatePrivateConnectionCertificate",
        "aidevops:UpdateRecommendation",
        "aidevops:UpdateTrigger",
        "aidevops:ValidateAwsAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AIDevOpsAgentReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke DevOps Agen Amazon melalui Konsol Manajemen AWS

`AIDevOpsAgentReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AIDevOpsAgentReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Maret 2026, 03:42 UTC
- Waktu teredit: 11 Juni 2026, 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/AIDevOpsAgentReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIDevOpsAgentReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aidevops:DescribePrivateConnection",
        "aidevops:DescribeServices",
        "aidevops:Get*",
        "aidevops:List*",
        "aidevops:SearchServiceAccessibleResource"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AIDevOpsChannelAccessPolicy

Deskripsi: Menyediakan akses ke obrolan dan mengelola investigasi melalui AWS DevOps Agen untuk Anda AgentSpaces

`AIDevOpsChannelAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AIDevOpsChannelAccessPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Agustus 2026, 21:07 UTC
- Waktu teredit: 26 Agustus 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AIDevOpsChannelAccessPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowChatActions",
      "Effect" : "Allow",
      "Action" : [
        "aidevops:CreateChat",
        "aidevops:SendMessage"
      ],
      "Resource" : "arn:aws:aidevops:*:*:agentspace/${aws:PrincipalTag/AgentSpaceId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AIDevOpsConstellationAccessPolicy

Deskripsi: Menyediakan izin yang diperlukan oleh AWS DevOps Agen untuk berkoordinasi dengan AgentSpaces terhubung melalui Konstelasi Ruang Agen.

`AIDevOpsConstellationAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AIDevOpsConstellationAccessPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Agustus 2026, 16:27 UTC
- Waktu teredit: 05 Agustus 2026, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AIDevOpsConstellationAccessPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConstellationCoordination",
      "Effect" : "Allow",
      "Action" : [
        "aidevops:GetAgentSpace",
        "aidevops:CreateBacklogTask",
        "aidevops:GetBacklogTask",
        "aidevops:ListBacklogTasks",
        "aidevops:GetAsset",
        "aidevops:GetAssetContent",
        "aidevops:GetAssetFile",
        "aidevops:ListAssets",
        "aidevops:ListAssetFiles",
```

```
        "aidevops:ListExecutions",
        "aidevops:ListJournalRecords"
      ],
      "Resource" : "arn:aws:aidevops:*:*:agentspace/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AIDevOpsOperatorAppAccessPolicy

Deskripsi: Menyediakan akses untuk menggunakan aplikasi web AWS DevOps operator untuk Ruang Agen.

`AIDevOpsOperatorAppAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AIDevOpsOperatorAppAccessPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Maret 2026, 03:42 UTC
- Waktu teredit: 10 September 2026, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/AIDevOpsOperatorAppAccessPolicy`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOperatorAgentSpaceActions",
      "Effect" : "Allow",
      "Action" : [
        "aidevops:CreateAccessToken",
        "aidevops:CreateAsset",
        "aidevops:CreateAssetFile",
        "aidevops:CreateBacklogTask",
        "aidevops:CreateChat",
        "aidevops:CreateKnowledgeItem",
        "aidevops:CreateTrigger",
        "aidevops:DeleteAsset",
        "aidevops:DeleteAssetFile",
        "aidevops:DeleteKnowledgeItem",
        "aidevops:DeleteTrigger",
        "aidevops:DescribeServices",
        "aidevops:DescribeSupportLevel",
        "aidevops:DiscoverTopology",
        "aidevops:EndChatForCase",
        "aidevops:GetAccessToken",
        "aidevops:GetAgentSpace",
        "aidevops:GetAsset",
        "aidevops:GetAssetContent",
        "aidevops:GetAssetFile",
        "aidevops:GetAssociation",
        "aidevops:GetBacklogTask",
        "aidevops:GetKnowledgeItem",
        "aidevops:GetRecommendation",
        "aidevops:GetTrigger",
        "aidevops:InitiateChatForCase",
        "aidevops:ListAccessTokens",
        "aidevops:ListAssetFiles",
        "aidevops:ListAssets",
        "aidevops:ListAssetTypes",
```

```
        "aidevops:ListAssetVersions",
        "aidevops:ListAssociations",
        "aidevops:ListBacklogTasks",
        "aidevops:ListChats",
        "aidevops:ListExecutions",
        "aidevops:ListGoals",
        "aidevops:ListJournalRecords",
        "aidevops:ListKnowledgeItems",
        "aidevops:ListKnowledgeItemVersions",
        "aidevops:ListPendingMessages",
        "aidevops:ListRecommendations",
        "aidevops:ListTriggers",
        "aidevops:ListWebhooks",
        "aidevops:RevokeAccessToken",
        "aidevops:RotateAccessToken",
        "aidevops:SendMessage",
        "aidevops:UpdateApprovalAction",
        "aidevops:UpdateAsset",
        "aidevops:UpdateAssetFile",
        "aidevops:UpdateBacklogTask",
        "aidevops:UpdateGoal",
        "aidevops:UpdateKnowledgeItem",
        "aidevops:UpdateRecommendation",
        "aidevops:UpdateTrigger"
      ],
      "Resource" : [
        "arn:aws:aidevops:*:*:agentspace/${aws:PrincipalTag/AgentSpaceId}",
        "arn:aws:aidevops:*:*:agentspace/${aws:PrincipalTag/AgentSpaceId}/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorAccountActions",
      "Effect" : "Allow",
      "Action" : [
        "aidevops:GetAccountUsage"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSupportOperatorActions",
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeCases",
        "support:DescribeServices",
        "support:InitiateChatForCase",
        "support:DescribeSupportLevel"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSecretsManagerOperatorActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowTranscribeOperatorActions",
      "Effect" : "Allow",
      "Action" : [
        "transcribe:StartStreamTranscriptionWebSocket"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AIDevOpsReleaseManagementVPCPolicy

Deskripsi: Memberikan izin bagi AWS DevOps Agen untuk membuat dan mengelola antarmuka jaringan di VPC Anda sehingga agen manajemen rilis dapat mengakses sumber daya pribadi

`AIDevOpsReleaseManagementVPCPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AIDevOpsReleaseManagementVPCPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Agustus 2026, 22:27 UTC
- Waktu teredit: 21 Agustus 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/AIDevOpsReleaseManagementVPCPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ManagedByVerificationTesting" : [
            ""
          ],
```

```
          "ec2:CreateAction" : "CreateNetworkInterface",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ManagedByVerificationTesting" : "",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "ManagedByVerificationTesting"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/ManagedByVerificationTesting" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AIOpsAssistantIncidentReportPolicy

Deskripsi: Memberikan izin yang diperlukan oleh Amazon AI Operations Assistant untuk menghasilkan laporan insiden penyelidikan.

`AIOpsAssistantIncidentReportPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AIOpsAssistantIncidentReportPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 Oktober 2025, 22:04 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsAssistantIncidentReportPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Statement1",
      "Effect" : "Allow",
```

```
      "Action" : [
        "aiops:PutFact",
        "aiops:UpdateReport",
        "aiops:GetReport",
        "aiops:GenerateReport",
        "aiops:CreateReport",
        "aiops:GetFact",
        "aiops:ListFacts",
        "aiops:GetFactVersions",
        "aiops:GetInvestigation",
        "aiops:ListInvestigationEvents",
        "aiops:GetInvestigationEvent"
      ],
      "Resource" : [
        "arn:aws:aiops:*:*:investigation-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : [
            "${aws:ResourceAccount}"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AIOpsAssistantPolicy

Deskripsi: Memberikan ReadOnly izin yang diperlukan oleh Asisten Operasi AI Amazon untuk melakukan analisis pada AWS sumber daya pelanggan selama penyelidikan.

`AIOpsAssistantPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AIOpsAssistantPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Desember 2024, 16:21 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsAssistantPolicy`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOPSServiceAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:List*",
        "acm-pca:Describe*",
        "acm-pca:GetCertificate",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:List*",
        "acm:DescribeCertificate",
        "acm:GetAccountConfiguration",
        "airflow:List*",
        "amplify:GetApp",
        "amplify:GetBranch",
```

```
        "amplify:GetDomainAssociation",
        "amplify:List*",
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:List*",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetEnvironment",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:List*",
        "appflow:Describe*",
        "appflow:List*",
        "application-autoscaling:Describe*",
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:List*",
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "apprunner:Describe*",
        "apprunner:List*",
        "appstream:Describe*",
        "appstream:List*",
        "appsync:GetApiAssociation",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
        "appsync:GetFunction",
        "appsync:GetGraphqlApi",
        "appsync:GetGraphqlApiEnvironmentVariables",
        "appsync:GetIntrospectionSchema",
        "appsync:GetResolver",
        "appsync:GetSourceApiAssociation",
        "appsync:List*",
        "aps:Describe*",
        "aps:List*",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:List*",
        "athena:GetCapacityAssignmentConfiguration",
        "athena:GetCapacityReservation",
        "athena:GetDataCatalog",
```

```
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:List*",
        "auditmanager:GetAssessment",
        "auditmanager:List*",
        "autoscaling:Describe*",
        "backup-gateway:GetHypervisor",
        "backup-gateway:List*",
        "backup:Describe*",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:List*",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:List*",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetDataSource",
        "bedrock:GetGuardrail",
        "bedrock:GetKnowledgeBase",
        "bedrock:List*",
        "budgets:Describe*",
        "budgets:List*",
        "ce:Describe*",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:List*",
        "chatbot:Describe*",
        "chatbot:GetMicrosoftTeamsChannelConfiguration",
        "chatbot:List*",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:List*",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
```

```
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:List*",
        "cloudformation:Describe*",
        "cloudformation:GetResource",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:List*",
        "cloudfront:Describe*",
        "cloudfront:GetCachePolicy",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetContinuousDeploymentPolicy",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetFunction",
        "cloudfront:GetKeyGroup",
        "cloudfront:GetMonitoringSubscription",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetOriginRequestPolicy",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:List*",
        "cloudtrail:Describe*",
        "cloudtrail:GetChannel",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetQueryResults",
        "cloudtrail:GetResourcePolicy",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents",
        "cloudtrail:StartQuery",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetInsightRuleReport",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricStream",
        "cloudwatch:GetService",
```

```
        "cloudwatch:GetServiceLevelObjective",
        "cloudwatch:List*",
        "codeartifact:Describe*",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:List*",
        "codebuild:BatchGetFleets",
        "codebuild:List*",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codedeploy:BatchGetDeployments",
        "codedeploy:BatchGetDeploymentTargets",
        "codedeploy:GetApplication",
        "codedeploy:GetDeploymentConfig",
        "codedeploy:List*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:List*",
        "codeguru-reviewer:Describe*",
        "codeguru-reviewer:List*",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:List*",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:GetSyncConfiguration",
        "codestar-connections:List*",
        "codestar-notifications:Describe*",
        "codestar-notifications:List*",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeRiskConfiguration",
        "cognito-idp:DescribeUserImportJob",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetLogDeliveryConfiguration",
        "cognito-idp:GetUICustomization",
```

```
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:GetWebACLForResource",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListTagsForResource",
        "comprehend:Describe*",
        "comprehend:List*",
        "config:Describe*",
        "config:GetStoredQuery",
        "config:List*",
        "connect:Describe*",
        "connect:GetTaskTemplate",
        "connect:List*",
        "databrew:Describe*",
        "databrew:List*",
        "datapipeline:Describe*",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:List*",
        "datasync:Describe*",
        "datasync:List*",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetLicenseEndpoint",
        "deadline:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetStorageProfile",
        "deadline:List*",
        "detective:GetMembers",
        "detective:List*",
        "devicefarm:GetDevicePool",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:GetVPCEConfiguration",
        "devicefarm:List*",
        "devops-guru:Describe*",
        "devops-guru:GetResourceCollection",
```

```
        "devops-guru:List*",
        "dms:Describe*",
        "dms:List*",
        "ds:Describe*",
        "dynamodb:Describe*",
        "dynamodb:GetResourcePolicy",
        "dynamodb:List*",
        "ec2:Describe*",
        "ec2:GetAssociatedEnclaveCertificateIamRoles",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayRoutes",
        "ecr:Describe*",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:List*",
        "ecs:Describe*",
        "ecs:List*",
        "eks:Describe*",
        "eks:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticfilesystem:Describe*",
        "elasticloadbalancing:GetResourcePolicy",
        "elasticloadbalancing:GetTrustStoreCaCertificatesBundle",
        "elasticloadbalancing:GetTrustStoreRevocationContent",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "emr-containers:Describe*",
        "emr-containers:List*",
```

```
        "emr-serverless:GetApplication",
        "emr-serverless:List*",
        "es:Describe*",
        "es:List*",
        "events:Describe*",
        "events:List*",
        "evidently:GetExperiment",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:List*",
        "firehose:Describe*",
        "firehose:List*",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:List*",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:List*",
        "forecast:Describe*",
        "forecast:List*",
        "frauddetector:BatchGetVariable",
        "frauddetector:Describe*",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModelVersion",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:List*",
        "fsx:Describe*",
        "gamelift:Describe*",
        "gamelift:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:GetDatabase",
        "glue:GetDatabases",
```

```
        "glue:GetJob",
        "glue:GetRegistry",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:List*",
        "glue:querySchemaVersionMetadata",
        "grafana:Describe*",
        "grafana:List*",
        "greengrass:Describe*",
        "greengrass:GetDeployment",
        "greengrass:List*",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:List*",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetIPSet",
        "guardduty:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:List*",
        "health:DescribeEvents",
        "health:DescribeEventDetails",
        "healthlake:Describe*",
        "healthlake:List*",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetLoginProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetUser",
        "iam:GetUserPolicy",
```

```
        "iam:ListAttachedRolePolicies",
        "iam:ListOpenIDConnectProviders",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListServerCertificates",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroups",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:GetWorkflow",
        "imagebuilder:List*",
        "inspector2:List*",
        "inspector:Describe*",
        "inspector:List*",
        "internetmonitor:GetMonitor",
        "internetmonitor:List*",
        "iot:Describe*",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetPolicy",
        "iot:GetThingShadow",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:GetV2LoggingOptions",
        "iot:List*",
        "iotanalytics:Describe*",
        "iotanalytics:List*",
        "iotevents:Describe*",
        "iotevents:List*",
        "iotfleethub:Describe*",
        "iotfleethub:List*",
        "iotsitewise:Describe*",
        "iotsitewise:List*",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
```

```
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:List*",
        "ivs:GetChannel",
        "ivs:GetEncoderConfiguration",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:List*",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:List*",
        "kafka:Describe*",
        "kafka:GetClusterPolicy",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kendra:Describe*",
        "kendra:List*",
        "kinesis:Describe*",
        "kinesis:GetResourcePolicy",
        "kinesis:List*",
        "kinesisanalytics:Describe*",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kms:DescribeKey",
        "kms:ListResourceTags",
        "kms:ListKeys",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeyRotations",
        "lakeformation:Describe*",
        "lakeformation:GetLFTag",
        "lakeformation:GetResourceLFTags",
        "lakeformation:List*",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
```

```
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:List*",
        "launchwizard:GetDeployment",
        "launchwizard:List*",
        "lex:Describe*",
        "lex:List*",
        "license-manager:GetLicense",
        "license-manager:List*",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:Describe*",
        "logs:FilterLogEvents",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:List*",
        "logs:StartQuery",
```

```
        "logs:StopLiveTail",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "lookoutmetrics:Describe*",
        "lookoutmetrics:List*",
        "lookoutvision:Describe*",
        "lookoutvision:List*",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:List*",
        "macie2:GetAllowList",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsFilter",
        "macie2:GetMacieSession",
        "macie2:List*",
        "mediaconnect:Describe*",
        "mediaconnect:List*",
        "medialive:Describe*",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:List*",
        "mediapackage-vod:Describe*",
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:List*",
        "memorydb:Describe*",
        "memorydb:List*",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:List*",
        "mq:Describe*",
        "mq:List*",
        "network-firewall:Describe*",
        "network-firewall:List*",
        "networkmanager:Describe*",
        "networkmanager:GetConnectAttachment",
```

```
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:List*",
        "nimble:GetLaunchProfile",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:List*",
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:List*",
        "omics:GetAnnotationStore",
        "omics:GetReferenceStore",
        "omics:GetRunGroup",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:List*",
        "opsworks-cm:Describe*",
        "opsworks-cm:List*",
        "organizations:Describe*",
        "organizations:List*",
        "osis:GetPipeline",
        "osis:List*",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:List*",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
```

```
        "pca-connector-ad:List*",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:List*",
        "personalize:Describe*",
        "personalize:List*",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics",
        "pipes:Describe*",
        "pipes:List*",
        "proton:GetEnvironmentTemplate",
        "proton:GetServiceTemplate",
        "proton:List*",
        "qbusiness:GetApplication",
        "qbusiness:GetDataSource",
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetRetriever",
        "qbusiness:GetWebExperience",
        "qbusiness:List*",
        "qldb:Describe*",
        "qldb:List*",
        "ram:GetPermission",
        "ram:List*",
        "rds:Describe*",
        "rds:List*",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
        "redshift:Describe*",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetRoute",
        "refactor-spaces:List*",
        "rekognition:Describe*",
        "rekognition:List*",
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:List*",
```

```
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:List*",
        "robomaker:Describe*",
        "robomaker:List*",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:List*",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:List*",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:List*",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetOutpostResolver",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:List*",
        "rum:GetAppMonitor",
        "rum:List*",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:List*",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
```

```
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointConfigurationForObjectLambda",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "S3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
        "s3:List*",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:List*",
        "schemas:Describe*",
        "schemas:GetResourcePolicy",
        "schemas:List*",
        "secretsmanager:Describe*",
```

```
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:List*",
        "securityhub:BatchGetAutomationRules",
        "securityhub:BatchGetSecurityControls",
        "securityhub:Describe*",
        "securityhub:GetConfigurationPolicy",
        "securityhub:GetConfigurationPolicyAssociation",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindingAggregator",
        "securityhub:GetInsights",
        "securityhub:List*",
        "securitylake:GetSubscriber",
        "securitylake:List*",
        "servicecatalog:Describe*",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:List*",
        "servicequotas:GetServiceQuota",
        "ses:Describe*",
        "ses:GetAccount",
        "ses:GetAddonInstance",
        "ses:GetAddonSubscription",
        "ses:GetArchive",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailIdentity",
        "ses:GetEmailTemplate",
        "ses:GetIngressPoint",
        "ses:GetRelay",
        "ses:GetRuleSet",
        "ses:GetTemplate",
        "ses:GetTrafficPolicy",
        "ses:List*",
        "shield:Describe*",
        "shield:List*",
        "signer:GetSigningProfile",
        "signer:List*",
        "sns:GetDataProtectionPolicy",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:List*",
```

```
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:List*",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:List*",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:List*",
        "ssm-sap:GetApplication",
        "ssm-sap:List*",
        "ssm:Describe*",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetParameters",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:List*",
        "sso-directory:SearchGroups",
        "sso-directory:SearchUsers",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetManagedApplicationInstance",
        "sso:GetPermissionsBoundaryForPermissionSet",
        "sso:GetSharedSsoConfiguration",
        "sso:ListAccountAssignments",
        "sso:ListApplicationAssignments",
        "sso:ListApplications",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListInstances",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListTagsForResource",
        "states:GetExecutionHistory",
        "states:Describe*",
        "states:List*",
        "synthetics:Describe*",
        "synthetics:GetCanary",
        "synthetics:GetGroup",
        "synthetics:List*",
        "tag:GetResources",
        "timestream:Describe*",
        "timestream:List*",
        "transfer:Describe*",
        "transfer:List*",
        "verifiedpermissions:GetIdentitySource",
```

```
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:List*",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetAuthPolicy",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:List*",
        "wafv2:GetIPSet",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRegexPatternSet",
        "wafv2:GetRuleGroup",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:List*",
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetUserSettings",
        "workspaces-web:List*",
        "workspaces:Describe*",
        "xray:BatchGetTraces",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:GetServiceGraph",
        "xray:GetTraceSummaries",
        "xray:List*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AIOPSS3AccessForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::amplify",
        "arn:aws:s3:::cdk--assets--*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ViaAWSService" : [
            "amplify.amazonaws.com"
          ],
          "aws:PrincipalAccount" : [
            "${aws:ResourceAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "AIOPSAPIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integrations",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integrations/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/stages",
```

```
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/domainnames/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AIOpsConsoleAdminPolicy

Deskripsi: Memberikan akses penuh ke layanan Amazon AI Operations dan izin yang diperlukan melalui AWS konsol. Ini juga mencakup izin untuk menggunakan sesi konsol yang sadar identitas.

`AIOpsConsoleAdminPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AIOpsConsoleAdminPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Desember 2024, 23:51 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsConsoleAdminPolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOpsAdmin",
      "Effect" : "Allow",
      "Action" : [
        "aiops:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOApplicationManagement",
      "Effect" : "Allow",
      "Action" : [
        "sso:PutApplicationAccessScope",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationGrant",
        "sso:PutApplicationAuthenticationMethod",
        "sso:DeleteApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "aiops.amazonaws.com",
          "aws:ResourceTag/ManagedByAmazonAIOperations" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "SSOApplicationTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication",
        "sso:TagResource"
      ],
      "Resource" : [
        "arn:aws:sso:::instance/*",
        "arn:aws:sso::aws:applicationProvider/aiops"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "aiops.amazonaws.com",
          "aws:RequestTag/ManagedByAmazonAIOperations" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ManagedByAmazonAIOperations"
          ]
        }
      }
    },
    {
      "Sid" : "SSOTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "sso:TagResource"
      ],
      "Resource" : "arn:aws:sso::*:application/*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "aiops.amazonaws.com",
          "aws:ResourceTag/ManagedByAmazonAIOperations" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ManagedByAmazonAIOperations"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "sso:ListApplications",
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:DescribeInstance",
        "sso:GetSSOStatus",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSTSContextSetting",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "IdentityPropagationAccess",
      "Effect" : "Allow",
      "Action" : [
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudtrailAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListTrails",
        "cloudtrail:DescribeTrails",
        "cloudtrail:ListEventDataStores"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMIntegrationSecretsManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:aws/ssm/3p/*"
    },
    {
      "Sid" : "SSMIntegrationAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetServiceSetting",
        "ssm:UpdateServiceSetting"
      ],
      "Resource" : "arn:aws:ssm:*:*:servicesetting/integrations/*"
    },
    {
      "Sid" : "SSMIntegrationCreatePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreatePolicy"
      ],
      "Resource" : "arn:aws:iam::*:policy/service-role/
AWSServiceRoleSSMIntegrationsPolicy*"
    },
    {
      "Sid" : "ChatbotConfigurations",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeChimeWebhookConfigurations",
        "chatbot:DescribeSlackWorkspaces",
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations",
        "chatbot:ListMicrosoftTeamsConfiguredTeams"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "IAMPassRoleToAIOps",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "aiops.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMListRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagBoundaryPermission",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassRoleToSSMIntegration",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.integrations.amazonaws.com"
        },
        "ArnEquals" : {
          "iam:AssociatedResourceArn" : "arn:aws:aiops:*:*:investigation-group/*"
        }
```

```
      }
    },
    {
      "Sid" : "SSMOpsItemAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:*:ssm:*:*:opsitem/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Integration" : "CloudWatch",
          "aws:ResourceTag/Integration" : "CloudWatch"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Integration"
          ]
        }
      }
    },
    {
      "Sid" : "CreateAIOpsCrossAccountAssistantPolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreatePolicy"
      ],
      "Resource" : "arn:aws:iam::*:policy/AIOpsCrossAccountAssistantPolicy*"
    },
    {
      "Sid" : "AmazonQAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
        "q:PassRequest"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AIOpsOperatorAccess

Deskripsi: Memberikan akses ke Amazon AI Operations API untuk membuat, memperbarui, dan menghapus investigasi, peristiwa investigasi, dan sumber daya investigasi. Ini juga mencakup ReadOnly akses ke semua API Operasi AI dan untuk menggunakan sesi yang sadar identitas.

`AIOpsOperatorAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AIOpsOperatorAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Desember 2024, 23:51 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsOperatorAccess`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOpsOperatorAccess",
      "Effect" : "Allow",
      "Action" : [
        "aiops:CreateInvestigation",
        "aiops:CreateInvestigationEvent",
        "aiops:CreateInvestigationResource",
        "aiops:DeleteInvestigation",
        "aiops:Get*",
        "aiops:List*",
        "aiops:UpdateInvestigation",
        "aiops:UpdateInvestigationEvent",
        "aiops:ValidateInvestigationGroup",
        "aiops:PutFact",
        "aiops:UpdateReport",
        "aiops:GenerateReport",
        "aiops:CreateReport",
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
        "q:PassRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "sso:DescribeInstance",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowSTSContextSetting",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "SSMSettingServiceIntegration",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetServiceSetting"
      ],
      "Resource" : "arn:aws:ssm:*:*:servicesetting/integrations/*"
    },
    {
      "Sid" : "SSMIntegrationTagAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Integration" : [
            "CloudWatch"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "Integration"
        }
      }
    },
    {
      "Sid" : "SSMOpsItemIntegration",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/Integration" : [
            "CloudWatch"
          ]
        }
      }
    },
    {
      "Sid" : "SSMTagOperation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Integration" : [
            "CloudWatch"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "Integration"
        }
      }
    },
    {
      "Sid" : "SSMOpsSummaryIntegration",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsSummary"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AIOpsReadOnlyAccess

Deskripsi: Mem ReadOnly berikan izin ke layanan Amazon AI Operations dan sumber daya yang diperlukan.

`AIOpsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AIOpsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Desember 2024, 23:51 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOpsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aiops:Get*",
        "aiops:List*",
        "aiops:ValidateInvestigationGroup"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "sso:DescribeInstance",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AlexaForBusinessDeviceSetup

Deskripsi: Menyediakan akses pengaturan perangkat ke AlexaForBusiness layanan

`AlexaForBusinessDeviceSetup`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AlexaForBusinessDeviceSetup` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2017, 16:47 UTC
- Waktu teredit: 20 Mei 2019, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:RegisterDevice",
        "a4b:CompleteRegistration",
        "a4b:SearchDevices",
        "a4b:SearchNetworkProfiles",
        "a4b:GetNetworkProfile",
        "a4b:PutDeviceSetupEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "A4bDeviceSetupAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:A4BNetworkProfile*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AlexaForBusinessFullAccess

Deskripsi: Memberikan akses penuh ke AlexaForBusiness sumber daya dan akses ke terkait Layanan AWS

`AlexaForBusinessFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AlexaForBusinessFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2017, 16:47 UTC
- Waktu teredit: 01 Juli 2020, 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:*",
        "kms:DescribeKey"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "*a4b.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*a4b.amazonaws.com/
AWSServiceRoleForAlexaForBusiness*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:A4B*"
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "A4B*"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AlexaForBusinessGatewayExecution

Deskripsi: Menyediakan akses eksekusi gateway ke AlexaForBusiness layanan

`AlexaForBusinessGatewayExecution`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AlexaForBusinessGatewayExecution` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2017, 16:47 UTC
- Waktu teredit: 30 November 2017, 16:47 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:Send*",
        "a4b:Get*"
      ],
      "Resource" : "arn:aws:a4b:*:*:gateway/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:dd-*",
        "arn:aws:sqs:*:*:sd-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:List*",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AlexaForBusinessLifesizeDelegatedAccessPolicy

Deskripsi: Menyediakan akses ke perangkat Lifesize AVS

`AlexaForBusinessLifesizeDelegatedAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AlexaForBusinessLifesizeDelegatedAccessPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Juni 2020, 19:46 UTC
- Waktu teredit: 12 Juni 2020, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessLifesizeDelegatedAccessPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "a4b:DisassociateDeviceFromRoom",
        "a4b:DeleteDevice",
        "a4b:UpdateDevice",
        "a4b:GetDevice"
      ],
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A2IWO7UEGWV4TL"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:RegisterAVSDevice"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "a4b:amazonId" : [
            "A2IWO7UEGWV4TL"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:SearchDevices"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "a4b:filters_deviceType" : [
            "*A2IWO7UEGWV4TL"
          ]
        },
        "Null" : {
          "a4b:filters_deviceType" : "false"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:AssociateDeviceWithRoom"
      ],
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A2IWO7UEGWV4TL",
        "arn:aws:a4b:us-east-1:*:room/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:GetRoom",
        "a4b:GetAddressBook",
        "a4b:SearchRooms",
        "a4b:CreateContact",
        "a4b:CreateRoom",
        "a4b:UpdateContact",
        "a4b:ListConferenceProviders",
        "a4b:DeleteRoom",
        "a4b:CreateAddressBook",
        "a4b:DisassociateContactFromAddressBook",
        "a4b:CreateConferenceProvider",
        "a4b:PutConferencePreference",
        "a4b:DeleteAddressBook",
        "a4b:AssociateContactWithAddressBook",
        "a4b:DeleteContact",
        "a4b:SearchProfiles",
        "a4b:UpdateProfile",
        "a4b:GetContact"
      ],
      "Resource" : "*"
    },
    {
      "Action" : [
        "kms:DescribeKey"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:kms:*:*:key/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AlexaForBusinessNetworkProfileServicePolicy

Deskripsi: Kebijakan ini memungkinkan Alexa for Business melakukan tugas otomatis yang dijadwalkan oleh profil jaringan Anda.

`AlexaForBusinessNetworkProfileServicePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 13 Maret 2019, 00:53 UTC
- Waktu teredit: 05 April 2019, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "A4bPcaTagAccess",
      "Action" : [
        "acm-pca:GetCertificate",
        "acm-pca:IssueCertificate",
        "acm-pca:RevokeCertificate"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/a4b" : "enabled"
        }
      }
    },
    {
      "Sid" : "A4bNetworkProfileAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:A4BNetworkProfile*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AlexaForBusinessPolyDelegatedAccessPolicy

Deskripsi: Menyediakan akses ke perangkat Poly AVS

`AlexaForBusinessPolyDelegatedAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AlexaForBusinessPolyDelegatedAccessPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 Oktober 2019, 19:48 UTC
- Waktu teredit: 16 Oktober 2019, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "a4b:DisassociateDeviceFromRoom",
        "a4b:DeleteDevice",
        "a4b:UpdateDevice",
        "a4b:GetDevice"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A238TWV36W3S92",
        "arn:aws:a4b:us-east-1:*:device/*/*:A1FUZ1SC53VJXD"
      ]
    },
    {
      "Action" : [
```

```
        "a4b:RegisterAVSDevice"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "a4b:amazonId" : [
            "A238TWV36W3S92",
            "A1FUZ1SC53VJXD"
          ]
        }
      }
    },
    {
      "Action" : [
        "a4b:SearchDevices"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "a4b:AssociateDeviceWithRoom"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A238TWV36W3S92",
        "arn:aws:a4b:us-east-1:*:device/*/*:A1FUZ1SC53VJXD",
        "arn:aws:a4b:us-east-1:*:room/*"
      ]
    },
    {
      "Action" : [
        "a4b:GetRoom",
        "a4b:SearchRooms",
        "a4b:CreateRoom",
        "a4b:GetProfile",
        "a4b:SearchSkillGroups",
        "a4b:DisassociateSkillGroupFromRoom",
        "a4b:AssociateSkillGroupWithRoom",
```

```
        "a4b:GetSkillGroup",
        "a4b:SearchProfiles",
        "a4b:GetAddressBook",
        "a4b:UpdateRoom"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AlexaForBusinessReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke AlexaForBusiness layanan

`AlexaForBusinessReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AlexaForBusinessReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2017, 16:47 UTC
- Waktu teredit: 20 November 2019, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:Get*",
        "a4b:List*",
        "a4b:Search*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonAPIGatewayAdministrator

Deskripsi: Menyediakan akses penuh ke create/edit /delete API di Amazon API Gateway melalui. Konsol Manajemen AWS

`AmazonAPIGatewayAdministrator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAPIGatewayAdministrator` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Juli 2015, 17:34 UTC
- Waktu teredit: 09 Juli 2015, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:*"
      ],
      "Resource" : "arn:aws:apigateway:*::/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonAPIGatewayInvokeFullAccess

Deskripsi: Menyediakan akses penuh untuk memanggil API di Amazon API Gateway.

`AmazonAPIGatewayInvokeFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAPIGatewayInvokeFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Juli 2015, 17:36 UTC
- Waktu teredit: 18 Desember 2018, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "execute-api:Invoke",
        "execute-api:ManageConnections"
      ],
      "Resource" : "arn:aws:execute-api:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonAPIGatewayPushToCloudWatchLogs

Deskripsi: Mengizinkan API Gateway untuk mendorong log ke akun pengguna.

`AmazonAPIGatewayPushToCloudWatchLogs`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAPIGatewayPushToCloudWatchLogs` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 November 2015, 23:41 UTC
- Waktu teredit: 11 November 2015, 23:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:FilterLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonAppFlowFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon AppFlow dan akses ke AWS layanan yang didukung sebagai sumber aliran atau tujuan (S3 dan Redshift). Juga menyediakan akses ke KMS untuk enkripsi

`AmazonAppFlowFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAppFlowFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Juni 2020, 23:30 UTC
- Waktu teredit: 28 Februari 2022, 23.11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "appflow:*",
      "Resource" : "*"
    },
    {
      "Sid" : "ListRolesForRedshift",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSListAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
```

```
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "KMSListGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3ReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "S3PutBucketPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::appflow-*"
    },
    {
      "Sid" : "SecretsManagerCreateSecretAccess",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "appflow!*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecretsManagerPutResourcePolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        },
        "StringEqualsIgnoreCase" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "appflow"
        }
      }
    },
    {
```

```
      "Sid" : "LambdaListFunctions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonAppFlowReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke alur Amazon Appflow

`AmazonAppFlowReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAppFlowReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Juni 2020, 23:26 UTC
- Waktu teredit: 28 Februari 2022, 20.42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeConnector",
        "appflow:DescribeConnectors",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlows",
        "appflow:DescribeFlowExecution",
        "appflow:DescribeConnectorFields",
        "appflow:ListConnectors",
        "appflow:ListConnectorFields",
        "appflow:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy

Deskripsi: Memberikan izin ke switch Wilayah ARC untuk pelaksanaan rencana dan evaluasi rencana.

`AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 November 2025, 19:34 UTC
- Waktu teredit: 02 Oktober 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "arc-region-switch:GetPlan",
        "arc-region-switch:GetPlanExecution",
        "arc-region-switch:ListPlanExecutions"
      ],
      "Resource" : "*",
      "Sid" : "GetPlanAndExecutions"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "iam:SimulatePrincipalPolicy",
      "Resource" : "arn:aws:iam::*:role/*",
      "Sid" : "PlanEvaluation"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*",
      "Sid" : "CloudWatch"
    },
    {
      "Sid" : "ServiceQuotasRead",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ServiceQuotasWrite",
      "Effect" : "Allow",
      "Action" : "servicequotas:RequestServiceQuotaIncrease",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonAppStreamFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon AppStream melalui Konsol Manajemen AWS.

`AmazonAppStreamFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAppStreamFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 28 Agustus 2020, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "appstream:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
```

```
    },
    {
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:DeleteScheduledAction"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "iam:ListRoles",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
```

```
      "Resource" : "arn:aws:iam::*:role/service-role/
ApplicationAutoScalingForAmazonAppStreamAccess",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appstream.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_AppStreamFleet",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "appstream.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonAppStreamPCAAccess

Deskripsi: Ak AppStream ses Amazon 2.0 ke AWS Certificate Manager Private CA di akun pelanggan untuk otentikasi berbasis sertifikat

`AmazonAppStreamPCAAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAppStreamPCAAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 24 Oktober 2022, 17:05 UTC
- Waktu teredit: 24 Oktober 2022, 17.05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "arn:*:acm-pca:*:*:*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/euc-private-ca" : "*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonAppStreamReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon AppStream melalui Konsol Manajemen AWS.

`AmazonAppStreamReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAppStreamReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "appstream:List*",
        "appstream:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonAppStreamServiceAccess

Deskripsi: Kebijakan default untuk peran AppStream layanan Amazon.

`AmazonAppStreamServiceAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAppStreamServiceAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 November 2016, 04:17 UTC
- Waktu teredit: 03 September 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints",
        "s3:ListAllMyBuckets",
        "ds:DescribeDirectories",
        "application-autoscaling:DescribeScalableTargets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:DeleteObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::appstream2-36fb080bb8-*",
        "arn:aws:s3:::appstream-app-settings-*",
        "arn:aws:s3:::appstream-logs-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonAthenaFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Athena dan akses cakupan ke dependensi yang diperlukan untuk mengaktifkan kueri, menulis hasil, dan manajemen data.

`AmazonAthenaFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAthenaFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2016, 16:46 UTC
- Waktu teredit: 12 Februari 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAthenaFullAccess`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BaseAthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseGluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
```

```
        "glue:BatchGetPartition",
        "glue:StartColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetCatalogImportStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseQueryResultsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-athena-query-results-*"
      ]
    },
    {
      "Sid" : "BaseAthenaExamplesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::athena-examples*"
      ]
    },
    {
      "Sid" : "BaseS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
```

```
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseSNSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseCloudWatchPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseDataZonePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "datazone:ListDomains",
        "datazone:ListProjects",
        "datazone:ListAccountEnvironments"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BasePricingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "pricing:GetProducts"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonAthenaServiceRolePolicy

Deskripsi: Mengizinkan akses ke sumber daya AWS layanan lain yang diperlukan untuk menjalankan Amazon Athena

`AmazonAthenaServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 14 November 2025, 22:34 UTC
- Waktu teredit: 14 November 2025, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonAthenaServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Athena",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonAugmentedAIFullAccess

Deskripsi: Menyediakan akses untuk melakukan semua operasi Sumber daya Amazon Augmented AI, termasuk FlowDefinitions, HumanTaskUis dan HumanLoops. Tidak mengizinkan akses untuk membuat FlowDefinitions terhadap tim kerja publik.

`AmazonAugmentedAIFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAugmentedAIFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 16:21 UTC
- Waktu teredit: 03 Desember 2019, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*HumanLoop",
        "sagemaker:*HumanLoops",
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions",
        "sagemaker:*HumanTaskUi",
        "sagemaker:*HumanTaskUis"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonAugmentedAIHumanLoopFullAccess

Deskripsi: Menyediakan akses untuk melakukan semua operasi pada HumanLoops.

`AmazonAugmentedAIHumanLoopFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAugmentedAIHumanLoopFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 16:20 UTC
- Waktu teredit: 03 Desember 2019, 16:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*HumanLoop",
        "sagemaker:*HumanLoops"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonAugmentedAIIntegratedAPIAccess

Deskripsi: Menyediakan akses untuk melakukan semua operasi Sumber daya Amazon Augmented AI, termasuk FlowDefinitions, HumanTaskUis dan HumanLoops. Juga menyediakan akses ke operasi layanan yang terintegrasi dengan Amazon Augmented AI.

`AmazonAugmentedAIIntegratedAPIAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAugmentedAIIntegratedAPIAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 April 2020, 20:47 UTC
- Waktu teredit: 22 April 2020, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*HumanLoop",
        "sagemaker:*HumanLoops",
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions",
        "sagemaker:*HumanTaskUi",
        "sagemaker:*HumanTaskUis"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "textract:AnalyzeDocument"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rekognition:DetectModerationLabels"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonAuroraDSQLConsoleFullAccess

Deskripsi: Menyediakan akses administratif penuh konsol ke Aurora DSQL

`AmazonAuroraDSQLConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAuroraDSQLConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2024, 15:36 UTC
- Waktu teredit: 13 Mei 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v16 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DsqlAllPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:PutClusterPolicy",
        "dsql:GetClusterPolicy",
        "dsql:DeleteClusterPolicy",
        "dsql:CreateCluster",
        "dsql:GetCluster",
        "dsql:UpdateCluster",
        "dsql:DeleteCluster",
        "dsql:ListClusters",
        "dsql:TagResource",
        "dsql:UntagResource",
        "dsql:ListTagsForResource",
        "dsql:DbConnectAdmin",
        "dsql:DbConnect",
        "dsql:PutMultiRegionProperties",
        "dsql:PutWitnessRegion",
        "dsql:AddPeerCluster",
        "dsql:RemovePeerCluster",
        "dsql:GetVpcEndpointServiceName",
        "dsql:StartBackupJob",
        "dsql:GetBackupJob",
        "dsql:StopBackupJob",
        "dsql:StartRestoreJob",
        "dsql:GetRestoreJob",
        "dsql:StopRestoreJob",
        "dsql:InjectError",
        "dsql:CreateStream",
```

```
        "dsql:DeleteStream",
        "dsql:GetStream",
        "dsql:ListStreams",
        "dsql:UpdateStream"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DsqlConsolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ValidatePolicy",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "cloudwatch:GetMetricData",
        "ec2:DescribeVpcEndpoints",
        "kms:ListAliases",
        "kms:DescribeKey",
        "cloudwatch:ListMetrics",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSCryptographicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:dsql:ClusterId"
        }
```

```
      }
    },
    {
      "Sid" : "CreateDsqlServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "dsql.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassRoleForChangeStreams",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "dsql.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonAuroraDSQLFullAccess

Deskripsi: Menyediakan akses administratif penuh ke Aurora DSQL

`AmazonAuroraDSQLFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAuroraDSQLFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2024, 15:36 UTC
- Waktu teredit: 13 Mei 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLFullAccess`

Versi kebijakan

Versi kebijakan: v16 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DsqlAllPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:PutClusterPolicy",
        "dsql:GetClusterPolicy",
        "dsql:DeleteClusterPolicy",
        "dsql:CreateCluster",
        "dsql:GetCluster",
        "dsql:UpdateCluster",
        "dsql:DeleteCluster",
        "dsql:ListClusters",
        "dsql:TagResource",
        "dsql:UntagResource",
        "dsql:ListTagsForResource",
        "dsql:DbConnectAdmin",
```

```
        "dsql:DbConnect",
        "dsql:PutMultiRegionProperties",
        "dsql:PutWitnessRegion",
        "dsql:AddPeerCluster",
        "dsql:RemovePeerCluster",
        "dsql:GetVpcEndpointServiceName",
        "dsql:StartBackupJob",
        "dsql:GetBackupJob",
        "dsql:StopBackupJob",
        "dsql:StartRestoreJob",
        "dsql:GetRestoreJob",
        "dsql:StopRestoreJob",
        "dsql:InjectError",
        "dsql:CreateStream",
        "dsql:DeleteStream",
        "dsql:GetStream",
        "dsql:ListStreams",
        "dsql:UpdateStream"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RelatedServicesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDsqlServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "dsql.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KMSDescribePermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForChangeStreams",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "dsql.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KMSCryptographicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:dsql:ClusterId"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonAuroraDSQLReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Aurora DSQL

`AmazonAuroraDSQLReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAuroraDSQLReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2024, 15:21 UTC
- Waktu teredit: 13 Mei 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DsqlReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetClusterPolicy",
        "dsql:GetCluster",
        "dsql:GetVpcEndpointServiceName",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
        "dsql:GetStream",
        "dsql:ListStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RelatedServicesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRo

Deskripsi: Memberikan izin inferensi Model Bedrock ke memori inti agen Bedrock

`AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: Juli 16, 2025, 13:37 UTC
- Waktu teredit: 17 Juli 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockInvokeModel",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
```

```
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockMantleInference",
      "Effect" : "Allow",
      "Action" : "bedrock-mantle:CreateInference",
      "Resource" : "arn:aws:bedrock-mantle:*:*:project/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockMantleCallWithBearerToken",
      "Effect" : "Allow",
      "Action" : "bedrock-mantle:CallWithBearerToken",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonBedrockExternalWebSearchFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Bedrock Web Search, termasuk pengambilan konten dari situs web eksternal di luar batas AWS jaringan.

`AmazonBedrockExternalWebSearchFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBedrockExternalWebSearchFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Agustus 2026, 16:57 UTC
- Waktu teredit: 03 Agustus 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockExternalWebSearchFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBedrockExternalWebSearchFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch",
        "bedrock-websearch:ExternalWebAccess"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonBedrockExternalWebSearchReadOnly

Deskripsi: Menyediakan akses read-only ke Amazon Bedrock Web Search, termasuk pengambilan konten dari situs web eksternal di luar batas jaringan. AWS

`AmazonBedrockExternalWebSearchReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBedrockExternalWebSearchReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Agustus 2026, 16:57 UTC
- Waktu teredit: 03 Agustus 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockExternalWebSearchReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBedrockExternalWebSearchReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch",
        "bedrock-websearch:ExternalWebAccess"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonBedrockFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Bedrock serta akses terbatas ke layanan terkait yang diperlukan olehnya

`AmazonBedrockFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBedrockFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Desember 2023, 15:47 UTC
- Waktu teredit: 04 Agustus 2026, 05:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockFullAccess`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAll",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockMantleAll",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockWebSearch",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    },
    {
      "Sid" : "DescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
```

```
      ],
      "Resource" : "arn:*:kms:*:::*"
    },
    {
      "Sid" : "APIsWithAllResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceModelEndpointMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com",
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointAddTagsOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
```

```
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker-sdk:bedrock",
            "bedrock:marketplace-registration-status",
            "sagemaker-studio:hub-content-arn"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/sagemaker-sdk:bedrock" : "compatible",
          "aws:RequestTag/bedrock:marketplace-registration-status" : "registered",
          "aws:RequestTag/sagemaker-studio:hub-content-arn" :
"arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointDeleteTagsOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker-sdk:bedrock",
            "bedrock:marketplace-registration-status",
            "sagemaker-studio:hub-content-arn"
          ]
        },
        "StringLike" : {
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible",
          "aws:ResourceTag/bedrock:marketplace-registration-status" : "registered",
          "aws:ResourceTag/sagemaker-studio:hub-content-arn" :
"arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*"
        }
```

```
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointNonMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:ListEndpoints",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointInvokingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com",
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible"
        }
      }
    },
    {
      "Sid" : "DiscoveringMarketplaceModel",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:DescribeHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*",
        "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
      ]
    },
    {
      "Sid" : "AllowMarketplaceModelsListing",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListHubContents"
      ],
      "Resource" : "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
    },
    {
      "Sid" : "PassRoleToSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*SageMaker*ForBedrock*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleToBedrock",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*AmazonBedrock*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
```

```
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrockFor3pModels",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonBedrockLimitedAccess

Deskripsi: Menyediakan akses terbatas ke Amazon Bedrock serta layanan terkait yang diperlukan olehnya

`AmazonBedrockLimitedAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBedrockLimitedAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 Juni 2025, 22:22 UTC
- Waktu teredit: 04 Agustus 2026, 05:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockLimitedAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAPIs",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:Get*",
        "bedrock:List*",
        "bedrock:CallWithBearerToken",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:CancelAutomatedReasoningPolicyBuildWorkflow",
        "bedrock:CreateAutomatedReasoningPolicy",
        "bedrock:CreateAutomatedReasoningPolicyTestCase",
        "bedrock:CreateAutomatedReasoningPolicyVersion",
        "bedrock:CreateEvaluationJob",
        "bedrock:CreateGuardrail",
        "bedrock:CreateGuardrailVersion",
        "bedrock:CreateInferenceProfile",
        "bedrock:CreateModelCopyJob",
        "bedrock:CreateModelCustomizationJob",
        "bedrock:CreateModelImportJob",
        "bedrock:CreateModelInvocationJob",
```

```
        "bedrock:CreatePromptRouter",
        "bedrock:CreateProvisionedModelThroughput",
        "bedrock:DeleteAutomatedReasoningPolicy",
        "bedrock:DeleteAutomatedReasoningPolicyBuildWorkflow",
        "bedrock:DeleteAutomatedReasoningPolicyTestCase",
        "bedrock:DeleteCustomModel",
        "bedrock:DeleteGuardrail",
        "bedrock:DeleteImportedModel",
        "bedrock:DeleteInferenceProfile",
        "bedrock:DeletePromptRouter",
        "bedrock:DeleteProvisionedModelThroughput",
        "bedrock:ExportAutomatedReasoningPolicyVersion",
        "bedrock:StartAutomatedReasoningPolicyBuildWorkflow",
        "bedrock:StartAutomatedReasoningPolicyTestWorkflow",
        "bedrock:StopEvaluationJob",
        "bedrock:StopModelCustomizationJob",
        "bedrock:StopModelInvocationJob",
        "bedrock:TagResource",
        "bedrock:UntagResource",
        "bedrock:UpdateAutomatedReasoningPolicy",
        "bedrock:UpdateAutomatedReasoningPolicyAnnotations",
        "bedrock:UpdateAutomatedReasoningPolicyTestCase",
        "bedrock:UpdateGuardrail",
        "bedrock:UpdateProvisionedModelThroughput",
        "bedrock:ApplyGuardrail",
        "bedrock:InvokeAutomatedReasoningPolicy",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:*:kms:*:::*"
    },
    {
      "Sid" : "APIsWithAllResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockMantleAPIs",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:Get*",
        "bedrock-mantle:List*",
        "bedrock-mantle:CreateInference"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockWebSearch",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrockFor3pModels",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : [
            "bedrock.amazonaws.com",
            "bedrock-mantle.amazonaws.com"
          ]
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonBedrockMantleFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Bedrock Mantle serta akses terbatas ke layanan terkait yang diperlukan olehnya

`AmazonBedrockMantleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBedrockMantleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Desember 2025, 07:19 UTC
- Waktu teredit: 04 Agustus 2026, 04:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMantleFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockMantleAll",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockWebSearch",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrockMantleFor3pModels",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock-mantle.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonBedrockMantleInferenceAccess

Deskripsi: Menyediakan akses pembuatan baca dan inferensi ke Amazon Bedrock Mantle

`AmazonBedrockMantleInferenceAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBedrockMantleInferenceAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Desember 2025, 07:19 UTC
- Waktu teredit: 04 Agustus 2026, 05:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMantleInferenceAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockMantleInference",
      "Effect" : "Allow",
```

```
      "Action" : [
        "bedrock-mantle:Get*",
        "bedrock-mantle:List*",
        "bedrock-mantle:CreateInference"
      ],
      "Resource" : "arn:aws:bedrock-mantle:*:*:project/*"
    },
    {
      "Sid" : "BedrockWebSearch",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    },
    {
      "Sid" : "BedrockMantleCallWithBearerToken",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:CallWithBearerToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrockMantleFor3pModels",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock-mantle.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonBedrockMantleReadOnly

Deskripsi: Menyediakan akses baca saja ke Amazon Bedrock Mantle

`AmazonBedrockMantleReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBedrockMantleReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Desember 2025, 07:19 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMantleReadOnly`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "BedrockMantleReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:Get*",
        "bedrock-mantle:List*"
      ],
      "Resource" : "arn:aws:bedrock-mantle:*:*:project/*"
    },
    {
      "Sid" : "BedrockMantleCallWithBearerToken",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:CallWithBearerToken"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonBedrockMarketplaceAccess

Deskripsi: Menyediakan akses terbatas ke Amazon Bedrock Marketplace serta layanan terkait yang diperlukan olehnya

`AmazonBedrockMarketplaceAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBedrockMarketplaceAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 Juni 2025, 22:22 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMarketplaceAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockMarketplaceAPIs",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateMarketplaceModelEndpoint",
        "bedrock:DeleteMarketplaceModelEndpoint",
        "bedrock:DeregisterMarketplaceModelEndpoint",
        "bedrock:RegisterMarketplaceModelEndpoint",
        "bedrock:UpdateMarketplaceModelEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceModelEndpointMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:DeleteEndpoint",
```

```
        "sagemaker:UpdateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com",
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointAddTagsOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker-sdk:bedrock",
            "bedrock:marketplace-registration-status",
            "sagemaker-studio:hub-content-arn"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/sagemaker-sdk:bedrock" : "compatible",
          "aws:RequestTag/bedrock:marketplace-registration-status" : "registered",
          "aws:RequestTag/sagemaker-studio:hub-content-arn" :
"arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointDeleteTagsOperations",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker-sdk:bedrock",
            "bedrock:marketplace-registration-status",
            "sagemaker-studio:hub-content-arn"
          ]
        },
        "StringLike" : {
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible",
          "aws:ResourceTag/bedrock:marketplace-registration-status" : "registered",
          "aws:ResourceTag/sagemaker-studio:hub-content-arn" :
"arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointNonMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:ListEndpoints",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointInvokingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com",
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible"
        }
      }
    },
    {
      "Sid" : "DiscoveringMarketplaceModel",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*",
        "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
      ]
    },
    {
      "Sid" : "AllowMarketplaceModelsListing",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListHubContents"
      ],
      "Resource" : "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
    },
    {
      "Sid" : "PassRoleToSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/*SageMaker*ForBedrock*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleToBedrock",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*AmazonBedrock*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonBedrockReadOnly

Deskripsi: Menyediakan akses baca saja ke Amazon Bedrock

`AmazonBedrockReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBedrockReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Desember 2023, 15:48 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockReadOnly`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBedrockReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:Get*",
        "bedrock:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceModelEndpointNonMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
```

```
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:ListEndpoints",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DiscoveringMarketplaceModel",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*",
        "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
      ]
    },
    {
      "Sid" : "AllowMarketplaceModelsListing",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListHubContents"
      ],
      "Resource" : "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonBedrockStudioPermissionsBoundary

Deskripsi: Mendefinisikan izin maksimum peran IAM yang dibuat Amazon Bedrock Studio untuk mengoperasikan sumber daya Amazon Bedrock Studio.

`AmazonBedrockStudioPermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBedrockStudioPermissionsBoundary` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Agustus 2024, 00:24 UTC
- Waktu teredit: 01 Agustus 2024, 00:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockStudioPermissionsBoundary`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessS3Buckets",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:DeleteObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::br-studio-${aws:PrincipalAccount}-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessOpenSearchCollections",
      "Effect" : "Allow",
      "Action" : "aoss:APIAccessAll",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "InvokeBedrockModels",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*::foundation-model/*"
    },
    {
      "Sid" : "AccessBedrockResources",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeAgent",
        "bedrock:Retrieve",
        "bedrock:StartIngestionJob",
        "bedrock:GetIngestionJob",
```

```
        "bedrock:ListIngestionJobs",
        "bedrock:ApplyGuardrail",
        "bedrock:ListPrompts",
        "bedrock:GetPrompt",
        "bedrock:CreatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:InvokeFlow",
        "bedrock:ListTagsForResource",
        "bedrock:TagResource",
        "bedrock:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RetrieveAndGenerate",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
      "Sid" : "WriteLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/br-studio-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "InvokeLambdaFunctions",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:br-studio-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AccessSecretsManagerSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:br-studio/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "UseKmsKeyWithBedrock",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/EnableBedrock" : "true"
        },
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:arn" : "false"
        }
      }
    },
    {
      "Sid" : "UseKmsKeyWithAwsServices",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/EnableBedrock" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonBedrockWebSearchFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Bedrock Web Search. Data tetap berada dalam batas AWS jaringan.

`AmazonBedrockWebSearchFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBedrockWebSearchFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Agustus 2026, 16:42 UTC
- Waktu teredit: 03 Agustus 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockWebSearchFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBedrockWebSearchFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonBedrockWebSearchReadOnly

Deskripsi: Menyediakan akses baca-saja ke Pencarian Web Amazon Bedrock. Data tetap berada dalam batas AWS jaringan.

`AmazonBedrockWebSearchReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBedrockWebSearchReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Agustus 2026, 16:57 UTC
- Waktu teredit: 03 Agustus 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockWebSearchReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBedrockWebSearchReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonBioDiscoveryFullAccess

Deskripsi: Memungkinkan akses administratif penuh ke Amazon Bio Discovery

`AmazonBioDiscoveryFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBioDiscoveryFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Agustus 2026, 06:27 UTC
- Waktu teredit: 18 Agustus 2026, 06:27 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonBioDiscoveryFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBioDiscoveryFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "researchstudio:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonBioDiscoveryPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "researchstudio.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonBioDiscoveryIdentityStoreAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
```

```
        "identitystore:ListUsers",
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser"
      ],
      "Resource" : [
        "arn:aws:identitystore::*:identitystore/*",
        "arn:aws:identitystore:::user/*",
        "arn:aws:identitystore:::group/*",
        "arn:aws:identitystore:::membership/*"
      ]
    },
    {
      "Sid" : "AmazonBioDiscoveryIdentityCenterAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication",
        "sso:CreateApplicationAssignment",
        "sso:DeleteApplication",
        "sso:DeleteApplicationAuthenticationMethod",
        "sso:DeleteApplicationGrant",
        "sso:DescribeApplication",
        "sso:DescribeApplicationAssignment",
        "sso:GetApplicationAuthenticationMethod",
        "sso:GetApplicationGrant",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationGrant",
        "sso:DeleteApplicationAssignment",
        "sso:DescribeInstance",
        "sso:ListInstances",
        "sso:ListApplications",
        "sso:ListApplicationAssignments",
        "sso:ListApplicationGrants",
        "sso:PutApplicationAccessScope",
        "sso:DeleteApplicationAccessScope",
        "sso:ListApplicationAccessScopes",
        "sso:DescribeRegisteredRegions"
      ],
      "Resource" : [
        "arn:aws:sso:::instance/*",
        "arn:aws:sso::*:application/*/*",
        "arn:aws:sso::aws:applicationProvider/ResearchStudio"
      ]
    },
    {
```

```
      "Sid" : "AmazonBioDiscoveryIdentityCenterKMSAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:aws:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonBioDiscoveryIdentityStoreKMSAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:aws:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonBioDiscoveryInAppFullAccess

Deskripsi: Menyediakan akses penuh ke tindakan dalam aplikasi Amazon Bio Discovery

`AmazonBioDiscoveryInAppFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBioDiscoveryInAppFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Agustus 2026, 06:47 UTC
- Waktu teredit: 18 Agustus 2026, 06:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBioDiscoveryInAppFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBioDiscoveryInAppFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "researchstudio:*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AmazonBioDiscoveryIdentityStoreInAppAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "arn:aws:identitystore::*:identitystore/*",
        "arn:aws:identitystore:::user/*",
        "arn:aws:identitystore:::group/*",
        "arn:aws:identitystore:::membership/*"
      ]
    },
    {
      "Sid" : "AmazonBioDiscoveryIdentityCenterInAppAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplicationAssignment",
        "sso:DeleteApplicationAssignment",
        "sso:ListApplicationAssignments"
      ],
      "Resource" : [
        "arn:aws:sso:::instance/*",
        "arn:aws:sso::*:application/*/*"
      ]
    },
    {
      "Sid" : "AmazonBioDiscoveryIdentityCenterKMSInAppAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:aws:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "AmazonBioDiscoveryIdentityStoreKMSInAppAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:aws:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonBraketFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Braket melalui Konsol Manajemen AWS dan SDK. Juga menyediakan akses ke layanan terkait (misalnya, S3, log).

`AmazonBraketFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBraketFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 06 Agustus 2020, 20:12 UTC
- Waktu teredit: 06 Juli 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketFullAccess`

Versi kebijakan

Versi kebijakan: v13 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::amazon-braket-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
```

```
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/AmazonBraket" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "servicequotas:GetServiceQuota",
        "cloudwatch:GetMetricData",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/amazon-braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
```

```
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListNotebookInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StopNotebookInstance",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:ListTags",
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance/amazon-braket-*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/amazon-
braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "braket:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/braket.amazonaws.com/
AWSServiceRoleForAmazonBraket*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "braket.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonBraketServiceSageMakerNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonBraketJobsExecutionRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "braket.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "/aws/braket"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonBraketJobsExecutionPolicy

Deskripsi: Memberikan akses Layanan AWS dan sumber daya yang diperlukan untuk menjalankan Amazon Braket Job termasuk S3, Cloudwatch, IAM, dan Braket

`AmazonBraketJobsExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBraketJobsExecutionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 November 2021, 19:34 UTC
- Waktu teredit: 06 Juli 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::amazon-braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/AmazonBraket" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/amazon-braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "braket:CancelJob",
        "braket:CancelQuantumTask",
        "braket:CreateJob",
        "braket:CreateQuantumTask",
        "braket:GetDevice",
        "braket:GetJob",
        "braket:GetQuantumTask",
        "braket:SearchDevices",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "braket:ListTagsForResource",
        "braket:TagResource",
        "braket:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonBraketJobsExecutionRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "braket.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:GetLogEvents",
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:StopQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "/aws/braket"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonBraketServiceRolePolicy

Deskripsi: Mengizinkan Amazon Braket membuat dan mengelola AWS sumber daya atas nama Anda

`AmazonBraketServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 04 Agustus 2020, 17:12 UTC
- Waktu teredit: 06 Juli 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::amazon-braket-*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/AmazonBraket" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonChimeFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Chime Admin Console melalui. Konsol Manajemen AWS

`AmazonChimeFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonChimeFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 November 2017, 22:15 UTC
- Waktu teredit: 14 Desember 2020, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
```

```
        "chime:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:ChimeVoiceConnector-Streaming*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:CreateQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"
      ]
    },
    {
      "Action" : [
        "kinesis:ListStreams"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream"
      ],
      "Resource" : [
        "arn:aws:kinesis:*:*:stream/chime-chat-*",
        "arn:aws:kinesis:*:*:stream/chime-messaging-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::chime-chat-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonChimeReadOnly

Deskripsi: Menyediakan akses baca saja ke Amazon Chime Admin Console melalui. Konsol Manajemen AWS

`AmazonChimeReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonChimeReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 November 2017, 22:04 UTC
- Waktu teredit: 14 Desember 2020, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeReadOnly`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "chime:List*",
```

```
        "chime:Get*",
        "chime:Describe*",
        "chime:SearchAvailablePhoneNumbers"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonChimeSDK

Deskripsi: Menyediakan akses ke operasi Amazon Chime SDK

`AmazonChimeSDK`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonChimeSDK` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Februari 2020, 21:53 UTC
- Waktu teredit: 10 Januari 2023, 18:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeSDK`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "chime:CreateMeeting",
        "chime:CreateMeetingWithAttendees",
        "chime:DeleteMeeting",
        "chime:GetMeeting",
        "chime:ListMeetings",
        "chime:CreateAttendee",
        "chime:BatchCreateAttendee",
        "chime:DeleteAttendee",
        "chime:GetAttendee",
        "chime:ListAttendees",
        "chime:ListAttendeeTags",
        "chime:ListMeetingTags",
        "chime:ListTagsForResource",
        "chime:TagAttendee",
        "chime:TagMeeting",
        "chime:TagResource",
        "chime:UntagAttendee",
        "chime:UntagMeeting",
        "chime:UntagResource",
        "chime:StartMeetingTranscription",
        "chime:StopMeetingTranscription",
        "chime:CreateMediaCapturePipeline",
        "chime:CreateMediaConcatenationPipeline",
        "chime:CreateMediaLiveConnectorPipeline",
        "chime:DeleteMediaCapturePipeline",
        "chime:DeleteMediaPipeline",
        "chime:GetMediaCapturePipeline",
        "chime:GetMediaPipeline",
        "chime:ListMediaCapturePipelines",
        "chime:ListMediaPipelines"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

Deskripsi: Kebijakan Terkelola Untuk Peran Terkait MediaPipelines Layanan Amazon Chime SDK

`AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 04 April 2022, 22:02 UTC
- Waktu teredit: 08 Desember 2023, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutMetricsForChimeSDKNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/ChimeSDK"
        }
      }
    },
    {
      "Sid" : "AllowKinesisVideoStreamsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia",
        "kinesisvideo:UpdateDataRetention",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:CreateStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/ChimeMediaPipelines-*"
      ]
    },
    {
      "Sid" : "AllowKinesisVideoStreamsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:ListStreams"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "AllowChimeMeetingAccess",
      "Effect" : "Allow",
      "Action" : [
        "chime:GetMeeting",
        "chime:CreateAttendee",
        "chime:DeleteAttendee"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonChimeSDKMessagingServiceRolePolicy

Deskripsi: Mengizinkan Amazon Chime SDK Messaging mengakses AWS sumber daya dan mengaktifkan fungsionalitas perpesanan

`AmazonChimeSDKMessagingServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 03 Maret 2023, 01:43 UTC
- Waktu teredit: 03 Maret 2023, 01:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "kinesis.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStream"
      ],
      "Resource" : [
        "arn:aws:kinesis:*:*:stream/chime-messaging-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonChimeServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Sumber AWS Daya yang digunakan atau dikelola oleh Amazon Chime

`AmazonChimeServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 30 September 2019, 22:25 UTC
- Waktu teredit: 30 September 2019, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/chime.amazonaws.com/
AWSServiceRoleForAmazonChime"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "chime.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonChimeTranscriptionServiceLinkedRolePolicy

Deskripsi: Mengizinkan Amazon Chime mengakses Amazon Transcribe dan Amazon Transcribe Medical atas nama Anda

`AmazonChimeTranscriptionServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 04 Agustus 2021, 21:47 UTC

- Waktu teredit: 04 Agustus 2021, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeTranscriptionServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:StartStreamTranscription",
        "transcribe:StartMedicalStreamTranscription"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonChimeUserManagement

Deskripsi: Menyediakan akses manajemen pengguna ke Amazon Chime Admin Console melalui. Konsol Manajemen AWS

`AmazonChimeUserManagement`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonChimeUserManagement` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 November 2017, 22:17 UTC
- Waktu teredit: 18 Februari 2020, 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeUserManagement`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "chime:ListAccounts",
        "chime:GetAccount",
        "chime:GetAccountSettings",
        "chime:UpdateAccountSettings",
        "chime:ListUsers",
        "chime:GetUser",
        "chime:GetUserByEmail",
        "chime:InviteUsers",
        "chime:InviteUsersFromProvider",
        "chime:SuspendUsers",
        "chime:ActivateUsers",
        "chime:UpdateUserLicenses",
        "chime:ResetPersonalPIN",
        "chime:LogoutUser",
```

```
        "chime:ListDomains",
        "chime:GetDomain",
        "chime:ListDirectories",
        "chime:ListGroups",
        "chime:SubmitSupportRequest",
        "chime:ListDelegates",
        "chime:ListAccountUsageReportData",
        "chime:GetMeetingDetail",
        "chime:ListMeetingEvents",
        "chime:ListMeetingsReportData",
        "chime:GetUserActivityReportData",
        "chime:UpdateUser",
        "chime:BatchUpdateUser",
        "chime:BatchSuspendUser",
        "chime:BatchUnsuspendUser",
        "chime:AssociatePhoneNumberWithUser",
        "chime:DisassociatePhoneNumberFromUser",
        "chime:GetPhoneNumber",
        "chime:ListPhoneNumbers",
        "chime:GetUserSettings",
        "chime:UpdateUserSettings",
        "chime:CreateUser",
        "chime:AssociateSigninDelegateGroupsWithAccount",
        "chime:DisassociateSigninDelegateGroupsFromAccount"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

Deskripsi: Kebijakan terkelola untuk Peran Tertaut Layanan untuk Amazon Chime VoiceConnector

`AmazonChimeVoiceConnectorServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 30 September 2019, 22:16 UTC
- Waktu teredit: 14 April 2023, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "chime:GetVoiceConnector*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia",
        "kinesisvideo:UpdateDataRetention",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:CreateStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/ChimeVoiceConnector-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:ListStreams"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:ChimeVoiceConnector-Streaming*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "chime:CreateMediaInsightsPipeline",
        "chime:GetMediaInsightsPipelineConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCloudDirectoryFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Cloud Directory Service.

`AmazonCloudDirectoryFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCloudDirectoryFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Februari 2017, 00:41 UTC
- Waktu teredit: 25 Februari 2017, 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "clouddirectory:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCloudDirectoryReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Cloud Directory Service.

`AmazonCloudDirectoryReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCloudDirectoryReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Februari 2017, 23:42 UTC
- Waktu teredit: 28 Februari 2017, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "clouddirectory:List*",
        "clouddirectory:Get*",
        "clouddirectory:LookupPolicy",
        "clouddirectory:BatchRead"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCloudWatchEvidentlyFullAccess

Deskripsi: Menyediakan akses penuh hanya ke Amazon CloudWatch Jelas. Juga menyediakan akses ke Amazon S3 terkait, Amazon SNS, Amazon CloudWatch, dan layanan terkait lainnya.

`AmazonCloudWatchEvidentlyFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCloudWatchEvidentlyFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2021, 15:10 UTC
- Waktu teredit: 29 November 2021, 15.10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "evidently:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchRUMEvidentlyRole-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:ListTagsForResource"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:TagResource",
        "cloudwatch:UnTagResource"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:Evidently-Alarm-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : [
```

```
        "arn:*:sns:*:*:Evidently-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCloudWatchEvidentlyReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Jel CloudWatch as

`AmazonCloudWatchEvidentlyReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCloudWatchEvidentlyReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2021, 15:08 UTC
- Waktu teredit: 29 November 2021, 15:08 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "evidently:GetExperiment",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCloudWatchEvidentlyServiceRolePolicy

Deskripsi: Mem CloudWatch ungkinkan Layanan Evidently untuk mengelola AWS Sumber Daya terkait atas nama pelanggan

`AmazonCloudWatchEvidentlyServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 13 September 2022, 17:25 UTC
- Waktu teredit: 13 September 2022, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "appconfig:StartDeployment",
      "Resource" : [
        "arn:aws:appconfig:*:*:application/*",
        "arn:aws:appconfig:*:*:deploymentstrategy/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/DeployedBy" : "Evidently"
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "appconfig:StartDeployment",
      "Resource" : "arn:aws:appconfig:*:*:application/*/configurationprofile/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/Owner" : "Evidently"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "appconfig:TagResource",
      "Resource" : "arn:aws:appconfig:*:*:application/*/environment/*/deployment/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/DeployedBy" : "Evidently"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "appconfig:StopDeployment",
      "Resource" : "arn:aws:appconfig:*:*:application/*"
    },
    {
      "Effect" : "Deny",
      "Action" : "appconfig:StopDeployment",
      "Resource" : "arn:aws:appconfig:*:*:application/*/environment/*/deployment/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/DeployedBy" : "Evidently"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "appconfig:ListDeployments",
```

```
      "Resource" : "arn:aws:appconfig:*:*:application/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCloudWatchRUMFullAccess

Deskripsi: Memberikan izin akses penuh untuk layanan Amazon CloudWatch RUM

`AmazonCloudWatchRUMFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCloudWatchRUMFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2021, 15:46 UTC
- Waktu teredit: 29 November 2021, 15.46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rum:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/rum.amazonaws.com/
AWSServiceRoleForRealUserMonitoring"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/RUM-Monitor*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "cognito-identity.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
```

```
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:CreateIdentityPool",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:SetIdentityPoolRoles"
      ],
      "Resource" : "arn:aws:cognito-identity:*:*:identitypool/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy",
        "logs:CreateLogStream"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*RUMService*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group::log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:describeCanaries",
        "synthetics:describeCanariesLastRun"
      ],
      "Resource" : "arn:aws:synthetics:*:*:canary:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCloudWatchRUMReadOnlyAccess

Deskripsi: Memberikan izin baca saja untuk layanan Amazon CloudWatch RUM

`AmazonCloudWatchRUMReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCloudWatchRUMReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 29 November 2021, 15:43 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:ListRumMetricsDestinations",
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetResourcePolicy",
        "rum:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:describeCanariesLastRun",
        "synthetics:describeCanaries"
      ],
      "Resource" : "arn:aws:synthetics:*:*:canary:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group::log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSummaries"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCloudWatchRUMServiceRolePolicy

Deskripsi: Memberikan izin kepada Amazon CloudWatch RUM Service untuk mempublikasikan data pemantauan ke AWS layanan terkait lainnya

`AmazonCloudWatchRUMServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 17 November 2021, 23:17 UTC
- Waktu teredit: 22 Februari 2023, 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : [
            "RUM/CustomMetrics/*",
            "AWS/RUM"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCodeCatalystFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon CodeCatalyst

`AmazonCodeCatalystFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCodeCatalystFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 April 2023, 16:50 UTC
- Waktu teredit: 20 April 2023, 16:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeCatalystResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "codecatalyst:*",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeCatalystAssociateIAMRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "codecatalyst.amazonaws.com",
            "codecatalyst-runner.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCodeCatalystReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon CodeCatalyst

`AmazonCodeCatalystReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCodeCatalystReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 April 2023, 16:49 UTC
- Waktu teredit: 20 April 2023, 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "codecatalyst:Get*",
        "codecatalyst:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCodeCatalystSupportAccess

Deskripsi: Mengiz CodeCatalyst inkan Amazon membuat, memperbarui, dan menyelesaikan AWS Dukungan kasus atas nama Anda.

`AmazonCodeCatalystSupportAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCodeCatalystSupportAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 April 2023, 12:34 UTC
- Waktu teredit: 20 April 2023, 12:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeAttachment",
        "support:DescribeCaseAttributes",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:DescribeIssueTypes",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeSupportLevel",
        "support:SearchForCases",
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:InitiateCallForCase",
        "support:InitiateChatForCase",
        "support:PutCaseAttributes",
        "support:RateCaseCommunication",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCodeGuruProfilerAgentAccess

Deskripsi: Menyediakan akses yang diperlukan oleh agen CodeGuru Amazon Profiler.

`AmazonCodeGuruProfilerAgentAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCodeGuruProfilerAgentAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Februari 2021, 22:11 UTC
- Waktu teredit: 05 Mei 2022 18.11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:ConfigureAgent",
        "codeguru-profiler:CreateProfilingGroup",
        "codeguru-profiler:PostAgentProfile"
      ],
      "Resource" : "arn:aws:codeguru-profiler:*:*:profilingGroup/*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCodeGuruProfilerFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon CodeGuru Profiler.

`AmazonCodeGuruProfilerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCodeGuruProfilerFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 10:13 UTC
- Waktu teredit: 15 Juli 2020, 03:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeguru-profiler:*",
        "iam:ListRoles",
        "iam:ListUsers",
        "sns:ListTopics",
        "codeguru:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/*AWSServiceRoleForCodeGuruProfiler*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "codeguru-profiler.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCodeGuruProfilerReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon CodeGuru Profiler.

`AmazonCodeGuruProfilerReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCodeGuruProfilerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 10:30 UTC
- Waktu teredit: 27 Juni 2020, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeguru:Get*",
        "codeguru-profiler:BatchGet*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:Get*",
        "codeguru-profiler:List*",
        "iam:ListRoles",
```

```
        "iam:ListUsers"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCodeGuruReviewerFullAccess

Deskripsi: Memberikan akses penuh ke Amazon CodeGuru Reviewer dan akses cakupan ke dependensi yang diperlukan.

`AmazonCodeGuruReviewerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCodeGuruReviewerFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 08:33 UTC
- Waktu teredit: 29 Agustus 2020, 04:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:*",
        "codeguru:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer"
    },
    {
      "Sid" : "CodeCommitAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "codecommit:ListRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeCommitTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:TagResource",
        "codecommit:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "codeguru-reviewer"
        }
      }
    },
    {
      "Sid" : "CodeConnectTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:TagResource",
        "codestar-connections:UntagResource",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "codeguru-reviewer"
        }
      }
    },
    {
      "Sid" : "CodeConnectManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codestar-connections:ListConnections",
        "codestar-connections:PassConnection"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "ForAllValues:StringEquals" : {
          "codestar-connections:ProviderAction" : [
            "ListRepositories",
            "ListOwners"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCodeGuruReviewerReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon CodeGuru Reviewer.

`AmazonCodeGuruReviewerReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCodeGuruReviewerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 08:48 UTC
- Waktu teredit: 29 Agustus 2020, 04:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruReviewerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru:Get*",
        "codeguru-reviewer:List*",
        "codeguru-reviewer:Describe*",
        "codeguru-reviewer:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCodeGuruReviewerServiceRolePolicy

Deskripsi: Peran terkait layanan yang diperlukan untuk Amazon CodeGuru Reviewer untuk mengakses sumber daya atas nama Anda.

`AmazonCodeGuruReviewerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 03 Desember 2019, 05:31 UTC
- Waktu teredit: 27 November 2020, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessCodeGuruReviewerEnabledRepositories",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GetRepository",
        "codecommit:GetBranch",
        "codecommit:DescribePullRequestEvents",
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetDifferences",
        "codecommit:GetPullRequest",
        "codecommit:ListPullRequests",
        "codecommit:PostCommentForPullRequest",
        "codecommit:GitPull",
        "codecommit:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/codeguru-reviewer" : "enabled"
        }
      }
    },
    {
      "Sid" : "AccessCodeGuruReviewerEnabledConnections",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "codestar-connections:ProviderAction" : [
            "ListBranches",
            "GetBranch",
            "ListRepositories",
            "ListOwners",
            "ListPullRequests",
            "GetPullRequest",
```

```
            "ListPullRequestComments",
            "ListPullRequestCommits",
            "ListCommitFiles",
            "ListBranchCommits",
            "CreatePullRequestDiffComment",
            "GitPull"
          ]
        },
        "Null" : {
          "aws:ResourceTag/codeguru-reviewer" : "false"
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsResourceCleanup",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowGuruS3GetObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::codeguru-reviewer-*",
        "arn:aws:s3:::codeguru-reviewer-*/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCodeGuruSecurityFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon CodeGuru Security.

`AmazonCodeGuruSecurityFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCodeGuruSecurityFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Mei 2023, 21:03 UTC
- Waktu teredit: 09 Mei 2023, 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruSecurityFullAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCodeGuruSecurityScanAccess

Deskripsi: Menyediakan akses yang diperlukan untuk bekerja dengan pemindaian Amazon CodeGuru Security.

`AmazonCodeGuruSecurityScanAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCodeGuruSecurityScanAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Mei 2023, 20:54 UTC
- Waktu teredit: 09 Mei 2023, 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruSecurityScanAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateScan",
        "codeguru-security:CreateUploadUrl",
        "codeguru-security:GetScan",
        "codeguru-security:GetFindings"
      ],
      "Resource" : "arn:aws:codeguru-security:*:*:scans/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCognitoDeveloperAuthenticatedIdentities

Deskripsi: Menyediakan akses ke Amazon Cognito API untuk mendukung identitas terautentikasi pengembang dari backend otentikasi Anda.

`AmazonCognitoDeveloperAuthenticatedIdentities`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCognitoDeveloperAuthenticatedIdentities` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Maret 2015, 17:22 UTC
- Waktu teredit: 24 Maret 2015, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoDeveloperAuthenticatedIdentities`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:GetOpenIdTokenForDeveloperIdentity",
        "cognito-identity:LookupDeveloperIdentity",
        "cognito-identity:MergeDeveloperIdentities",
        "cognito-identity:UnlinkDeveloperIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCognitoIdpEmailServiceRolePolicy

Deskripsi: Mengizinkan layanan Amazon Cognito User Pools menggunakan identitas SES Anda untuk pengiriman email

`AmazonCognitoIdpEmailServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 21 Maret 2019, 21:32 UTC
- Waktu teredit: 21 Maret 2019, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ses:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCognitoIdpServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Kumpulan Pengguna Amazon Cognito

`AmazonCognitoIdpServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 26 Juni 2020, 22:30 UTC
- Waktu teredit: 26 Juni 2020, 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCognitoPowerUser

Deskripsi: Menyediakan akses administratif ke sumber daya Amazon Cognito yang ada. Anda memerlukan hak istimewa Akun AWS admin untuk membuat sumber daya Cognito baru.

`AmazonCognitoPowerUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCognitoPowerUser` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Maret 2015, 17:14 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoPowerUser`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:*",
        "cognito-idp:*",
        "cognito-sync:*",
        "iam:ListRoles",
        "iam:ListOpenIdConnectProviders",
        "iam:GetRole",
```

```
        "iam:ListSAMLProviders",
        "iam:GetSAMLProvider",
        "kinesis:ListStreams",
        "lambda:GetPolicy",
        "lambda:ListFunctions",
        "sns:GetSMSSandboxAccountStatus",
        "sns:ListPlatformApplications",
        "ses:ListIdentities",
        "ses:GetIdentityVerificationAttributes",
        "mobiletargeting:GetApps",
        "acm:ListCertificates",
        "sms-voice:DescribeAccountAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "cognito-idp.amazonaws.com",
            "email.cognito-idp.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/cognito-idp.amazonaws.com/
AWSServiceRoleForAmazonCognitoIdp*",
        "arn:aws:iam::*:role/aws-service-role/email.cognito-idp.amazonaws.com/
AWSServiceRoleForAmazonCognitoIdpEmail*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCognitoReadOnly

Deskripsi: Menyediakan akses baca saja ke sumber daya Amazon Cognito.

`AmazonCognitoReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCognitoReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Maret 2015, 17:06 UTC
- Waktu teredit: 01 Agustus 2019, 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoReadOnly`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:Describe*",
        "cognito-identity:Get*",
        "cognito-identity:List*",
        "cognito-idp:Describe*",
        "cognito-idp:AdminGet*",
        "cognito-idp:AdminList*",
        "cognito-idp:List*",
        "cognito-idp:Get*",
        "cognito-sync:Describe*",
        "cognito-sync:Get*",
        "cognito-sync:List*",
        "iam:ListOpenIdConnectProviders",
        "iam:ListRoles",
        "sns:ListPlatformApplications"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCognitoUnAuthedIdentitiesSessionPolicy

Deskripsi: Kebijakan ini menentukan kumpulan izin yang diizinkan untuk identitas yang tidak diautentikasi untuk Cognito Identity Pools. Kebijakan ini tidak dimaksudkan untuk digunakan sebagai kebijakan izin yang berdiri sendiri. Ini digunakan sebagai pagar pembatas terhadap kebijakan yang terlalu permisif yang dilampirkan untuk peran dalam kumpulan identitas. Jangan melampirkan kebijakan ini ke peran apa pun, karena Cognito Identity Service akan secara otomatis menyertakannya sebagai kebijakan cakupan saat membuat kredenSIAL. Hak istimewa untuk mengakses AWS sumber daya lain sementara melalui alur yang disempurnakan sekarang akan

ditentukan oleh persimpangan peran yang terkait dengan identitas pengguna yang tidak diautentikasi yang disediakan oleh layanan, dan hak istimewa yang diberikan dalam kebijakan terkelola ini yang dimiliki oleh Cognito.

`AmazonCognitoUnAuthedIdentitiesSessionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCognitoUnAuthedIdentitiesSessionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Juli 2023, 23:04 UTC
- Waktu teredit: 01 Mei 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnAuthedIdentitiesSessionPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CognitoUnAuthedIdentitiesSessionPolicy",
      "Effect" : "Allow",
      "Action" : [
        "rum:PutRumEvents",
        "sagemaker:InvokeEndpoint",
        "polly:*",
        "comprehend:*",
```

```
        "translate:*",
        "transcribe:*",
        "rekognition:*",
        "mobiletargeting:*",
        "firehose:*",
        "personalize:*",
        "geo:GetMap*",
        "geo:ListMaps",
        "geo:SearchPlaceIndex*",
        "geo:GetPlace",
        "geo:CalculateRoute*",
        "geo:*Geofence",
        "geo:*Geofences",
        "geo:*DevicePosition*",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyPair",
        "kms:GenerateDataKeyPairWithoutPlaintext",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonCognitoUnauthenticatedIdentities

Deskripsi: Kebijakan ini menentukan kumpulan izin yang diizinkan untuk identitas yang tidak diautentikasi untuk Cognito Identity Pools. Ini tidak perlu dilampirkan ke peran unauth Anda, karena Cognito Identity Service akan secara otomatis menyertakannya sebagai kebijakan cakupan saat

membuat kredenSIAL. Hak istimewa untuk mengakses AWS sumber daya lain sementara melalui alur yang disempurnakan sekarang akan ditentukan oleh persimpangan peran yang terkait dengan identitas pengguna yang tidak diautentikasi yang disediakan oleh layanan, dan hak istimewa yang diberikan dalam kebijakan terkelola ini yang dimiliki oleh Cognito.

`AmazonCognitoUnauthenticatedIdentities`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonCognitoUnauthenticatedIdentities` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Februari 2023, 22:36 UTC
- Waktu teredit: 01 Februari 2023, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "rum:PutRumEvents",
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonConnect_FullAccess

Deskripsi: Tujuan kebijakan ini adalah untuk memberikan izin kepada pengguna AWS Connect yang diperlukan untuk menggunakan sumber daya Connect. Kebijakan ini menyediakan akses penuh ke sumber daya AWS Connect melalui Konsol Connect dan API publik

`AmazonConnect_FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonConnect_FullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 November 2020, 19:54 UTC
- Waktu teredit: 07 Maret 2023, 14:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnect_FullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "connect:*",
        "ds:CreateAlias",
        "ds:AuthorizeApplication",
        "ds:CreateIdentityPoolDirectory",
        "ds:DeleteDirectory",
        "ds:DescribeDirectories",
        "ds:UnauthorizeApplication",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lex:GetBots",
        "lex:ListBots",
        "lex:ListBotAliases",
        "logs:CreateLogGroup",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "lambda:ListFunctions",
        "ds:CheckAlias",
        "profile:ListAccountIntegrations",
        "profile:GetDomain",
        "profile:ListDomains",
        "profile:GetProfileObjectType",
        "profile:ListProfileObjectTypeTemplates"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "profile:AddProfileKey",
        "profile:CreateDomain",
        "profile:CreateProfile",
```

```
        "profile:DeleteDomain",
        "profile:DeleteIntegration",
        "profile:DeleteProfile",
        "profile:DeleteProfileKey",
        "profile:DeleteProfileObject",
        "profile:DeleteProfileObjectType",
        "profile:GetIntegration",
        "profile:GetMatches",
        "profile:GetProfileObjectType",
        "profile:ListIntegrations",
        "profile:ListProfileObjects",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "profile:MergeProfiles",
        "profile:PutIntegration",
        "profile:PutProfileObject",
        "profile:PutProfileObjectType",
        "profile:SearchProfiles",
        "profile:TagResource",
        "profile:UntagResource",
        "profile:UpdateDomain",
        "profile:UpdateProfile"
      ],
      "Resource" : "arn:aws:profile:*:*:domains/amazon-connect-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketAcl"
      ],
      "Resource" : "arn:aws:s3:::amazon-connect-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "arn:aws:servicequotas:*:*:connect/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "connect.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:DeleteServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/
AWSServiceRoleForAmazonConnect*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/profile.amazonaws.com/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "profile.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonConnectCampaignsServiceLinkedRolePolicy

Deskripsi: Kebijakan untuk peran terkait layanan Amazon Connect Campaigns

`AmazonConnectCampaignsServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 23 September 2021, 20:54 UTC
- Waktu teredit: 18 Juni 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectCampaignsServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConnectCampaignAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect-campaigns:ListCampaigns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConnectCampaignsMetricsAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect:GetMetricDataV2"
      ],
```

```
      "Resource" : "arn:aws:connect-campaigns:*:*:campaign/*"
    },
    {
      "Sid" : "ConnectAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect:BatchPutContact",
        "connect:StopContact",
        "connect:DescribeContactFlow",
        "connect:SendOutboundEmail",
        "connect:SendOutboundWebNotification"
      ],
      "Resource" : "arn:aws:connect:*:*:instance/*"
    },
    {
      "Sid" : "ConnectChatAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect:SendOutboundChatMessage"
      ],
      "Resource" : [
        "arn:aws:connect:*:*:instance/*",
        "arn:aws:connect:*:*:phone-number/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSocialMessagingSendMessageOperations",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:SendWhatsAppMessage"
      ],
      "Resource" : "arn:aws:social-messaging:*:*:phone-number-id/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "AllowSocialMessagingTemplateOperations",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:GetWhatsAppMessageTemplate"
      ],
      "Resource" : "arn:aws:social-messaging:*:*:waba/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSMSVoiceOperationsForConnect",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:SendTextMessage"
      ],
      "Resource" : "arn:aws:sms-voice:*:*:phone-number/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EventBridgeListRuleAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:ListRules"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EventBridgeManagedResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
```

```
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/ConnectCampaignsRule*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "events:ManagedBy" : "connect-campaigns.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventBridgeListTargetsByRuleAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/ConnectCampaignsRule*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowWisdomForConnectCampaignsEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:GetMessageTemplate",
        "wisdom:RenderMessageTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectCampaignsEnabled" : "True"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonConnectReadOnlyAccess

Deskripsi: Memberikan izin untuk melihat instans Amazon Connect di Akun AWS.

`AmazonConnectReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonConnectReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Oktober 2018, 21:00 UTC
- Waktu teredit: 19 Juni 2024, 15:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowConnectReadOnly",
      "Effect" : "Allow",
```

```
      "Action" : [
        "connect:Get*",
        "connect:Describe*",
        "connect:List*",
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyConnectEmergencyAccess",
      "Effect" : "Deny",
      "Action" : "connect:AdminGetEmergencyAccessToken",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonConnectServiceLinkedRolePolicy

Deskripsi: Mengizinkan Amazon Connect membuat dan mengelola AWS sumber daya atas nama Anda.

`AmazonConnectServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 07 September 2018, 00:21 UTC

- Waktu teredit: 02 Oktober 2026, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v56 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowConnectActions",
      "Effect" : "Allow",
      "Action" : [
        "connect:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDeleteSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/
AWSServiceRoleForAmazonConnect_*"
    },
    {
      "Sid" : "AllowS3ObjectForConnectBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
```

```
        "s3:GetObjectAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-connect-*/*"
      ]
    },
    {
      "Sid" : "AllowGetBucketMetadataForConnectBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-connect-*"
      ]
    },
    {
      "Sid" : "AllowConnectLogGroupAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/connect/*:*"
      ]
    },
    {
      "Sid" : "AllowListLexBotAccess",
      "Effect" : "Allow",
      "Action" : [
        "lex:ListBots",
        "lex:ListBotAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCustomerProfilesForConnectDomain",
      "Effect" : "Allow",
```

```
      "Action" : "profile:*",
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*",
        "arn:aws:profile:*:*:/domains/amazon-connect-*",
        "arn:aws:profile:*:*:/templates*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowCustomerProfilesListOperations",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListRecommenderRecipes",
        "profile:ListAccountIntegrations",
        "profile:ListDomains"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DenyCustomerProfilesForConnectDomain",
      "Effect" : "Deny",
      "Action" : [
        "profile:CreateDomain",
        "profile:UpdateDomain",
        "profile:DeleteDomain",
        "profile:CreateEventStream",
        "profile:DeleteEventStream",
        "profile:DeleteWorkflow",
        "profile:DeleteProfileKey",
        "profile:UntagResource",
        "profile:TagResource",
        "profile:CreateIntegrationWorkflow"
      ],
      "Resource" : "arn:aws:profile:*:*:domains/*"
    },
```

```
    {
      "Sid" : "AllowAppIntegrationsForConnectEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "app-integrations:GetDataIntegration",
        "app-integrations:ListDataIntegrationAssociations",
        "app-integrations:CreateDataIntegrationSchedule",
        "app-integrations:StartDataIntegrationExecution",
        "app-integrations:ListDataIntegrationExecutions",
        "app-integrations:GetDataIntegrationExecution",
        "app-integrations:ListDataIntegrationSchedules",
        "app-integrations:UpdateDataIntegrationSchedule",
        "app-integrations:GetDataIntegrationSchedule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowWisdomForConnectEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "DenyWisdomForConnectEnabledTaggedResources",
      "Effect" : "Deny",
      "Action" : [
        "wisdom:DeleteAssistant",
        "wisdom:DeleteKnowledgeBase"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowListOperationForWisdom",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:ListAssistants",
        "wisdom:ListKnowledgeBases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKMSListRetirableGrants",
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowPutMetricsForConnectNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Connect"
        }
      }
    },
    {
      "Sid" : "AllowSMSVoiceOperationsForConnect",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:SendTextMessage",
        "sms-voice:DescribePhoneNumbers"
      ],
      "Resource" : "arn:aws:sms-voice:*:*:phone-number/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowCognitoForConnectEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPool",
        "cognito-idp:ListUserPoolClients"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowChimeSDKVoiceConnectorGetOperationForConnect",
      "Effect" : "Allow",
      "Action" : [
        "chime:GetVoiceConnector"
      ],
      "Resource" : "arn:aws:chime:*:*:vc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowChimeSDKVoiceConnectorListOperationForConnect",
      "Effect" : "Allow",
      "Action" : [
        "chime:ListVoiceConnectors"
      ],
      "Resource" : "arn:aws:chime:*:*:vc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "SESPermissionsForManagingReceiptRules",
      "Effect" : "Allow",
      "Action" : [
        "ses:DescribeReceiptRule",
        "ses:UpdateReceiptRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SESPermissionForManagingConnectProvidedSESIdentity",
      "Effect" : "Allow",
      "Action" : [
        "ses:DeleteEmailIdentity"
      ],
      "Resource" : "arn:aws:ses:*:*:identity/*.email.connect.aws*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SESConfigurationSetPermissionsForSendingEmail",
      "Effect" : "Allow",
      "Action" : [
        "ses:SendRawEmail"
      ],
      "Resource" : "arn:aws:ses:*:*:configuration-set/configuration-set-for-connect-DO-
NOT-DELETE",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "PassRoleToSESForReceiptRuleManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonConnectEmailSESAccessRole"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ses.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSocialMessagingOperations",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:SendWhatsAppMessage",
        "social-messaging:PostWhatsAppMessageMedia",
        "social-messaging:GetWhatsAppMessageMedia",
        "social-messaging:GetLinkedWhatsAppBusinessAccountPhoneNumber",
        "social-messaging:SendWhatsAppCallEvent"
      ],
      "Resource" : "arn:aws:social-messaging:*:*:phone-number-id/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowRetrievalOfWabas",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:ListLinkedWhatsAppBusinessAccounts"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "AllowRetrievalOfWhatsAppTemplates",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:GetWhatsAppMessageTemplate",
        "social-messaging:ListWhatsAppMessageTemplates"
      ],
      "Resource" : "arn:aws:social-messaging:*:*:waba/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowMobileTargetingOperationsForConnect",
      "Effect" : "Allow",
      "Action" : "mobiletargeting:SendMessages",
      "Resource" : "arn:aws:mobiletargeting:*:*:apps/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowPollyActions",
      "Effect" : "Allow",
      "Action" : [
        "polly:ListLexicons",
        "polly:DescribeVoices",
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonConnectSynchronizationServiceRolePolicy

Deskripsi: Mengizinkan Amazon Connect menyinkronkan AWS sumber daya di seluruh wilayah atas nama Anda.

`AmazonConnectSynchronizationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 27 Oktober 2023, 22:38 UTC
- Waktu teredit: 21 November 2025, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "AllowConnectActions",
      "Effect" : "Allow",
      "Action" : [
        "connect:Create*",
        "connect:BatchCreate*",
        "connect:Update*",
        "connect:BatchUpdate*",
        "connect:Delete*",
        "connect:BatchDelete*",
        "connect:Describe*",
        "connect:BatchDescribe*",
        "connect:List*",
        "connect:Search*",
        "connect:Associate*",
        "connect:Disassociate*",
        "connect:Get*",
        "connect:BatchGet*",
        "connect:Import*",
        "connect:TagResource",
        "connect:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DisallowedConnectActions",
      "Effect" : "Deny",
      "Action" : [
        "connect:Start*",
        "connect:Stop*",
        "connect:Resume*",
        "connect:Suspend*",
        "connect:*Contact",
        "connect:SearchContacts",
        "connect:*ContactAttributes*",
        "connect:*RealtimeContact*",
        "connect:*AnalyticsData*",
        "connect:*MetricData*",
        "connect:*UserData*",
        "connect:*ContactEvaluation",
        "connect:*AttachedFile*",
        "connect:UpdateContactSchedule",
        "connect:UpdateContactRoutingData",
        "connect:ListContactReferences",
```

```
        "connect:CreateParticipant",
        "connect:CreatePersistentContactAssociation",
        "connect:CreateInstance",
        "connect:DeleteInstance",
        "connect:ListInstances",
        "connect:ReplicateInstance",
        "connect:GetFederationToken",
        "connect:ClaimPhoneNumber",
        "connect:ImportPhoneNumber",
        "connect:ReleasePhoneNumber",
        "connect:SearchAvailablePhoneNumbers",
        "connect:CreateTrafficDistributionGroup",
        "connect:DeleteTrafficDistributionGroup",
        "connect:GetTrafficDistribution",
        "connect:UpdateTrafficDistribution"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPutMetricsForConnectNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Connect"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonConnectVoiceIDFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Connect Voice ID

`AmazonConnectVoiceIDFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonConnectVoiceIDFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 September 2021, 19:04 UTC
- Waktu teredit: 26 September 2021, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "voiceid:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDataZoneBedrockModelConsumptionPolicy

Deskripsi: Memberikan izin untuk menggunakan model Amazon Bedrock, termasuk memanggil profil inferensi aplikasi Amazon Bedrock yang dibuat untuk domain Amazon tertentu. DataZone

`AmazonDataZoneBedrockModelConsumptionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneBedrockModelConsumptionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 12 November 2024, 22:15 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneBedrockModelConsumptionPolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InvokeDomainInferenceProfiles",
      "Effect" : "Allow",
      "Action" : [
```

```
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneDomain" : "${datazone:domainId}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "ListFoundationModels",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockCreateSessionWithTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateSession",
        "bedrock:TagResource"
      ],
      "Resource" : "arn:aws:bedrock:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/AmazonDataZoneUser" : "${datazone:userId}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${datazone:userId}",
          "aws:RequestTag/AmazonDataZoneDomain" : "${datazone:domainId}",
          "aws:ResourceTag/AmazonDataZoneDomain" : "${datazone:domainId}"
        },
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneUser" : "",
          "aws:ResourceTag/AmazonDataZoneUser" : "",
          "aws:RequestTag/AmazonDataZoneDomain" : "",
          "aws:ResourceTag/AmazonDataZoneDomain" : ""
        },
```

```
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "AmazonDataZone*"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "BedrockSessionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetSession",
        "bedrock:UpdateSession",
        "bedrock:DeleteSession",
        "bedrock:EndSession",
        "bedrock:CreateInvocation",
        "bedrock:ListInvocations",
        "bedrock:PutInvocationStep",
        "bedrock:GetInvocationStep",
        "bedrock:ListInvocationSteps",
        "bedrock:ListTagsForResource"
      ],
      "Resource" : "arn:aws:bedrock:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${datazone:userId}",
          "aws:ResourceTag/AmazonDataZoneDomain" : "${datazone:domainId}"
        },
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "",
          "aws:ResourceTag/AmazonDataZoneDomain" : ""
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "BedrockListSessionsPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ListSessions",
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDataZoneBedrockModelManagementPolicy

Deskripsi: Memberikan izin untuk mengelola akses model Amazon Bedrock, termasuk membuat, menandai, dan menghapus profil inferensi aplikasi.

`AmazonDataZoneBedrockModelManagementPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneBedrockModelManagementPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 12 November 2024, 22:14 UTC
- Waktu teredit: 12 November 2024, 22:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneBedrockModelManagementPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageApplicationInferenceProfile",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile",
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneProject"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteApplicationInferenceProfile",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:DeleteInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "CreateApplicationInferenceProfileUsingFoundationModels",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
      ]
    },
    {
      "Sid" : "CreateApplicationInferenceProfileUsingBedrockModels",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDataZoneDomainExecutionRolePolicy

Deskripsi: Kebijakan default untuk peran DomainExecutionRole layanan Amazon DataZone. Peran ini digunakan oleh Amazon DataZone untuk membuat katalog, menemukan, mengatur, berbagi, dan menganalisis data di DataZone domain Amazon.

`AmazonDataZoneDomainExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneDomainExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 27 September 2023, 21:55 UTC
- Waktu teredit: 26 Februari 2026, 00:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v13 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DomainExecutionRoleStatement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:AddEntityOwner",
        "datazone:AddPolicyGrant",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetFilter",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateDataProduct",
        "datazone:CreateDataProductRevision",
        "datazone:CreateDataSource",
        "datazone:CreateDomainUnit",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateRule",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetFilter",
        "datazone:DeleteAssetType",
        "datazone:DeleteDataProduct",
        "datazone:DeleteDataSource",
        "datazone:DeleteDomainUnit",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteRule",
```

```
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
        "datazone:DeleteTimeSeriesDataPoints",
        "datazone:GetAsset",
        "datazone:GetAssetFilter",
        "datazone:GetAssetType",
        "datazone:GetDataProduct",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetLineageNode",
        "datazone:GetListing",
        "datazone:GetMetadataGenerationRun",
        "datazone:GetProject",
        "datazone:GetRule",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetTimeSeriesDataPoint",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetFilters",
        "datazone:ListAssetRevisions",
        "datazone:ListDataProductRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
```

```
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListLineageNodeHistory",
        "datazone:ListMetadataGenerationRuns",
        "datazone:ListNotifications",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListRules",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:ListWarehouseMetadata",
        "datazone:QueryGraph",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RemoveEntityOwner",
        "datazone:RemovePolicyGrant",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateDataSource",
        "datazone:UpdateDomainUnit",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
```

```
        "datazone:UpdateRule",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMResourceShareStatement",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShareAssociations",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDataZoneEnvironmentRolePermissionsBoundary

Deskripsi: DataZone Amazon membuat peran IAM untuk Lingkungan untuk melakukan tindakan analisis data, dan menggunakan kebijakan ini saat membuat peran ini untuk menentukan batas izin mereka.

`AmazonDataZoneEnvironmentRolePermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneEnvironmentRolePermissionsBoundary` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 11 September 2023, 23:38 UTC
- Waktu teredit: 17 November 2023, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneEnvironmentRolePermissionsBoundary`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateGlueConnection",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      }
    },
    {
      "Sid" : "GlueOperations",
      "Effect" : "Allow",
      "Action" : [
        "glue:*DataQuality*",
```

```
        "glue:BatchCreatePartition",
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
```

```
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "glue.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "SameAccountKmsOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KmsOperationsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:Verify",
        "kms:Sign"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AnalyticsOperations",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*",
        "sqlworkbench:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QueryOperations",
```

```
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
```

```
        "ec2:Describe*",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetWorkflows",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:SearchTables",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateDatabase",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "iam:GetRole",
        "iam:GetRolePolicy",
```

```
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListUsers",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeMetricFilters",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:GetLogRecord",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift:CreateClusterUser",
        "redshift:DescribeClusters",
        "redshift:DescribeDataShares",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:JoinGroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "secretsmanager:ListSecrets",
        "tag:GetResources"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "QueryOperationsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryResultsStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsManagerOperationsWithTagKeys",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AmazonDataZoneDomain" : "*",
          "aws:ResourceTag/AmazonDataZoneProject" : "*"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        }
      }
    },
    {
      "Sid" : "DataZoneS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
```

```
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/datazone/*"
      ]
    },
    {
      "Sid" : "DataZoneS3BucketLocation",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListDataZoneS3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "*/datazone/*",
            "datazone/*"
          ]
        }
      }
    },
    {
      "Sid" : "NotDeniedOperations",
      "Effect" : "Deny",
      "NotAction" : [
        "datazone:*",
        "sqlworkbench:*",
```

```
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "ec2:CreateNetworkInterface",
        "ec2:CreateTags",
        "ec2:DeleteNetworkInterface",
```

```
        "ec2:DeleteTags",
        "ec2:Describe*",
        "glue:*DataQuality*",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetWorkflows",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
```

```
        "glue:NotifyEvent",
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:List*",
        "iam:PassRole",
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ListKeys",
        "kms:Verify",
        "kms:Sign",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
```

```
        "logs:GetQueryResults",
        "logs:GetLogRecord",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift:CreateClusterUser",
        "redshift:DescribeClusters",
        "redshift:DescribeDataShares",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:JoinGroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets",
        "secretsmanager:TagResource",
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDataZoneFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon DataZone melalui Konsol Manajemen AWS serta akses terbatas ke layanan terkait yang diperlukan olehnya.

`AmazonDataZoneFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 September 2023, 20:06 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullAccess`

Versi kebijakan

Versi kebijakan: v13 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "sso:DescribeRegisteredRegions",
        "s3:ListAllMyBuckets",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "secretsmanager:ListSecrets",
        "iam:ListUsers",
        "glue:GetDatabases",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codewhisperer:ListProfiles",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListFoundationModels",
        "bedrock:ListTagsForResource",
        "aoss:ListSecurityPolicies"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "BucketReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "CreateBucketStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-datazone*",
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "ConfigureBucketStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketCORS",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RamCreateResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "datazone:Domain"
        }
      }
    },
    {
      "Sid" : "RamResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:RejectResourceShareInvitation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "RamResourceReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations",
        "ram:ListResourceSharePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RamAssociateResourceSharePermissionStatement",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:PermissionArn" : [
```

```
            "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionAmazonDataZoneDomain",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionAmazonDataZoneDomainFullAccessWithPortalAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceWithPortalAccess"
          ]
        }
      }
    },
    {
      "Sid" : "IAMPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMGetPolicyStatement",
      "Effect" : "Allow",
      "Action" : "iam:GetPolicy",
      "Resource" : [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneRedshiftAccessPolicy*"
      ]
    },
    {
      "Sid" : "DataZoneTagOnCreateDomainProjectTags",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
```

```
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "DataZoneTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "CreateSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "ConnectionStatement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "TagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:TagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "for-use-with-all-datazone-projects"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "UntagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UntagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "for-use-with-all-datazone-projects"
        }
      }
    },
    {
```

```
      "Sid" : "SSMParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParametersByPath",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/profiles*"
      ]
    },
    {
      "Sid" : "UseKMSKeyPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "true"
        },
        "Null" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetSecurityPolicy",
        "aoss:CreateSecurityPolicy"
      ],
      "Resource" : [
        "*"
```

```
      ],
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "genai-studio-*"
        }
      }
    },
    {
      "Sid" : "GetFoundationModelStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
      ]
    },
    {
      "Sid" : "GetInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*",
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ]
    },
    {
      "Sid" : "ApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "TagApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:DeleteInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDataZoneFullUserAccess

Deskripsi: Menyediakan akses penuh ke Amazon DataZone, tetapi tidak mengizinkan pengelolaan domain, pengguna, atau akun terkait.

`AmazonDataZoneFullUserAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneFullUserAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 September 2023, 21:06 UTC
- Waktu teredit: 19 November 2024, 21:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneUserOperations",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
```

```
        "datazone:AcceptSubscriptionRequest",
        "datazone:AddEntityOwner",
        "datazone:AddPolicyGrant",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetFilter",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateDataProduct",
        "datazone:CreateDataProductRevision",
        "datazone:CreateDataSource",
        "datazone:CreateDomainUnit",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateRule",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetFilter",
        "datazone:DeleteAssetType",
        "datazone:DeleteDataProduct",
        "datazone:DeleteDataSource",
        "datazone:DeleteDomainUnit",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteRule",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
```

```
        "datazone:DeleteTimeSeriesDataPoints",
        "datazone:GetAsset",
        "datazone:GetAssetFilter",
        "datazone:GetAssetType",
        "datazone:GetDataProduct",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetIamPortalLoginUrl",
        "datazone:GetLineageNode",
        "datazone:GetListing",
        "datazone:GetMetadataGenerationRun",
        "datazone:GetProject",
        "datazone:GetRule",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetTimeSeriesDataPoint",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetFilters",
        "datazone:ListAssetRevisions",
        "datazone:ListDataProductRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
```

```
        "datazone:ListGroupsForUser",
        "datazone:ListLineageNodeHistory",
        "datazone:ListMetadataGenerationRuns",
        "datazone:ListNotifications",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListRules",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:ListWarehouseMetadata",
        "datazone:PostTimeSeriesDataPoints",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RemoveEntityOwner",
        "datazone:RemovePolicyGrant",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateDataSource",
        "datazone:UpdateDomainUnit",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
        "datazone:UpdateRule",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "RAMResourceShareOperations",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShareAssociations",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDataZoneGlueManageAccessRolePolicy

Deskripsi: Kebijakan ini memberikan izin untuk mengiz DataZone inkan Amazon mengaktifkan penerbitan dan akses hibah ke data.

`AmazonDataZoneGlueManageAccessRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneGlueManageAccessRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 September 2023, 20:21 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneGlueManageAccessRolePolicy`

Versi kebijakan

Versi kebijakan: v18 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueTagDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringLikeIfExists" : {
          "aws:TagKeys" : "DataZoneDiscoverable_*"
        }
      }
    },
    {
      "Sid" : "GlueDataQuality",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListDataQualityResults",
        "glue:GetDataQualityResult"
      ],
      "Resource" : "arn:aws:glue:*:*:dataQualityRuleset/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "GlueCrawler",
      "Effect" : "Allow",
      "Action" : "glue:ListCrawls",
      "Resource" : "arn:aws:glue:*:*:crawler/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueConnection",
      "Effect" : "Allow",
      "Action" : "glue:GetConnection",
      "Resource" : [
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueTableDatabaseCatalog",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:GetDatabases",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:CreateCatalog",
        "glue:CreateDatabase",
        "glue:DeleteCatalog",
        "glue:DeleteDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
```

```
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:userDefinedFunction/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueGetTags",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTags",
        "glue:GetCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LakeformationResourceSharing",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:CreateDataCellsFilter",
        "lakeformation:CreateLakeFormationOptIn",
        "lakeformation:DeleteDataCellsFilter",
        "lakeformation:DeleteLakeFormationOptIn",
        "lakeformation:GrantPermissions",
        "lakeformation:GetDataCellsFilter",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListLakeFormationOptIns",
        "lakeformation:ListPermissions",
        "lakeformation:RegisterResource",
```

```
        "lakeformation:RevokePermissions",
        "lakeformation:UpdateDataCellsFilter",
        "glue:GetDatabase",
        "glue:GetTable",
        "organizations:DescribeOrganization",
        "ram:GetResourceShareInvitations",
        "ram:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LakeformationResourceFederatedSharing",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "lakeformation:GlueARN" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceSharing",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteResourcePolicy",
        "glue:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountLakeFormationResourceSharing",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceShareInvitation",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share-invitation/*"
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingViaLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DeleteResourceShare",
        "ram:DisassociateResourceShare",
        "ram:ListResourceSharePermissions",
```

```
        "ram:UpdateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetResourceSharesViaLakeFormation",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShares",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingViaLakeFormationHybrid",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ram:PermissionArn" : "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "KMSDecrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/datazone:projectId" : "proj-all"
        }
      }
    },
    {
      "Sid" : "GetRoleForDataZone",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/AmazonSageMakerManageAccess*",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerManageAccess*"
      ]
    },
    {
      "Sid" : "PassRoleForDataLocationRegistration",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/AmazonSageMakerManageAccess*",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerManageAccess*",
        "arn:aws:iam::*:role/datazone_usr_role*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lakeformation.amazonaws.com",
```

```
            "glue.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateCatalogEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateCatalogS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging"
      ],
      "Resource" : "arn:aws:s3:::redshift-staging-bucket*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDataZonePortalFullAccessPolicy

Deskripsi: Menyediakan akses penuh ke Amazon DataZone API

`AmazonDataZonePortalFullAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZonePortalFullAccessPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Maret 2023, 18:24 UTC
- Waktu teredit: 26 Maret 2023, 18:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : "datazonecontrol:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDataZonePreviewConsoleFullAccess

Deskripsi: Menyediakan akses penuh ke rilis Pratinjau Amazon DataZone melalui Konsol Manajemen AWS. Juga menyediakan akses pilihan ke layanan terkait lainnya.

`AmazonDataZonePreviewConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZonePreviewConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Maret 2023, 15:16 UTC
- Waktu teredit: 13 Juli 2023, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "datazonecontrol:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "glue:GetConnections",
        "glue:GetDatabase",
        "redshift:DescribeClusters",
        "ec2:DescribeSubnets",
        "secretsmanager:ListSecrets",
        "iam:ListRoles",
        "sso:DescribeRegisteredRegions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/AmazonDataZone-*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetPolicy",
      "Resource" : [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneBootstrapServicePolicy-
AmazonDataZoneBootstrapRole",
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneServicePolicy-
AmazonDataZoneServiceRole"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZoneServiceRole*",
        "arn:aws:iam::*:role/service-role/AmazonDataZoneServiceRole*",
        "arn:aws:iam::*:role/AmazonDataZoneBootstrapRole*",
        "arn:aws:iam::*:role/service-role/AmazonDataZoneBootstrapRole",
        "arn:aws:iam::*:role/AmazonDataZoneDomainExecutionRole",
        "arn:aws:iam::*:role/service-role/AmazonDataZoneDomainExecutionRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazonecontrol.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDataZoneProjectDeploymentPermissionsBoundary

Deskripsi: Amazon DataZone membuat peran IAM yang digunakan untuk menyebarkan proyek analisis data. DataZone menggunakan kebijakan ini saat membuat peran ini untuk menentukan batas izin mereka.

`AmazonDataZoneProjectDeploymentPermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneProjectDeploymentPermissionsBoundary` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Maret 2023, 02:54 UTC
- Waktu teredit: 04 April 2023, 02:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectDeploymentPermissionsBoundary`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/*datazone*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonDataZoneProjectRolePermissionsBoundary"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateKey",
        "kms:TagResource",
        "athena:CreateWorkGroup",
        "athena:TagResource",
        "iam:TagRole",
        "iam:TagPolicy",
        "logs:CreateLogGroup",
        "logs:TagLogGroup",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "datazone:*"
        },
```

```
        "StringLike" : {
          "aws:ResourceTag/datazone:projectId" : "proj-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteWorkGroup",
        "kms:ScheduleKeyDeletion",
        "kms:DescribeKey",
        "kms:EnableKeyRotation",
        "kms:DisableKeyRotation",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:Decrypt",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/datazone:projectId" : "proj-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "datazone:projectId"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeletePolicy",
        "s3:DeleteBucket"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:policy/datazone*",
        "arn:aws:s3:::datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter*",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/*datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetRolePolicy",
        "iam:CreatePolicy",
        "iam:ListPolicyVersions",
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:ListPermissions",
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabases",
        "glue:GetDatabase",
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/*datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:DeleteBucketPolicy",
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketAcl",
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging",
        "s3:PutBucketLogging",
        "s3:GetObject*",
        "s3:GetBucket*",
        "s3:List*",
        "s3:GetEncryptionConfiguration",
        "s3:DeleteObject*",
        "s3:PutObject*",
        "s3:Abort*"
      ],
      "Resource" : "arn:aws:s3:::*datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:Get*",
        "athena:List*",
        "ec2:CreateSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup",
        "ec2:Describe*",
        "ec2:Get*",
        "ec2:List*",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogGroups",
```

```
        "logs:DeleteLogGroup",
        "logs:DeleteRetentionPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:PutKeyPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : [
            "com.amazonaws.*.logs",
            "com.amazonaws.*.s3",
            "com.amazonaws.*.glue",
            "com.amazonaws.*.athena"
          ]
        }
      }
    },
    {
      "Action" : [
        "cloudformation:DescribeStacks",
```

```
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
        "cloudformation:DescribeChangeSet",
        "cloudformation:CreateChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:TagResource",
        "cloudformation:GetTemplateSummary"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "s3:GetObject*",
        "s3:GetBucket*",
        "s3:List*",
        "s3:GetEncryptionConfiguration",
        "s3:DeleteObject*",
        "s3:PutObject*",
        "s3:Abort*",
        "s3:DeleteBucket"
      ],
      "NotResource" : [
        "arn:aws:s3:::*datazone*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "kms:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Effect" : "Deny",
      "NotAction" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:AddTagsToResource",
        "ssm:GetParameters",
        "ssm:GetParameter",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:DeleteBucketPolicy",
        "s3:CreateBucket",
        "s3:PutBucketAcl",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging",
        "s3:ListBucket",
        "s3:PutBucketLogging",
        "s3:DeleteBucket",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:CreatePolicy",
        "iam:ListPolicyVersions",
        "iam:DeletePolicy",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
        "cloudformation:DescribeChangeSet",
        "cloudformation:CreateChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:TagResource",
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplateSummary",
        "athena:*",
        "kms:*",
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabases",
        "glue:GetDatabase",
```

```
        "lambda:*",
        "ec2:*",
        "logs:*",
        "servicecatalog:CreateApplication",
        "servicecatalog:DeleteApplication",
        "servicecatalog:GetApplication",
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy",
        "iam:UntagRole",
        "iam:PassRole",
        "iam:TagRole",
        "s3:GetBucket*",
        "s3:GetObject*",
        "s3:Abort*",
        "s3:GetEncryptionConfiguration",
        "s3:PutObject*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDataZoneProjectRolePermissionsBoundary

Deskripsi: DataZone Amazon membuat peran IAM untuk proyek untuk melakukan tindakan analisis data, dan menggunakan kebijakan ini saat membuat peran ini untuk menentukan batas izin mereka.

`AmazonDataZoneProjectRolePermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneProjectRolePermissionsBoundary` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Maret 2023, 02:51 UTC
- Waktu teredit: 21 Maret 2023, 02:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:List*",
        "s3:Get*",
        "s3:DeleteObjectVersion",
        "s3:RestoreObject",
        "s3:ReplicateObject",
```

```
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutObjectRetention",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:List*",
        "s3:Get*",
        "kms:List*",
        "kms:Get*",
        "kms:Describe*",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "logs:*",
        "athena:TerminateSession",
        "athena:CreatePreparedStatement",
        "athena:StopCalculationExecution",
        "athena:StartQueryExecution",
        "athena:UpdatePreparedStatement",
        "athena:BatchGet*",
```

```
        "athena:List*",
        "athena:UpdateNotebook",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:UpdateNotebookMetadata",
        "athena:DeleteNamedQuery",
        "athena:Get*",
        "athena:UpdateNamedQuery",
        "athena:CreateNamedQuery",
        "athena:ExportNotebook",
        "athena:StopQueryExecution",
        "athena:StartCalculationExecution",
        "athena:StartSession",
        "athena:CreatePresignedNotebookUrl",
        "athena:CreateNotebook",
        "athena:ImportNotebook",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "lakeformation:GetDataAccess",
        "lakeformation:BatchGrantPermissions",
        "lakeformation:GrantPermissions",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "ram:CreateResourceShare",
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:AcceptResourceShareInvitation",
        "ram:Get*",
        "ram:List*",
        "redshift:DescribeClusters",
        "redshift:JoinGroup",
        "redshift:CreateClusterUser",
        "redshift:GetClusterCredentials",
        "redshift-data:*",
        "redshift:AuthorizeDataShare",
        "redshift:DescribeDataShares",
        "redshift:AssociateDataShareConsumer",
        "tag:GetResources",
        "iam:ListRoles",
```

```
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "glue:CreateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateDataQualityRuleset",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateWorkflow",
        "sqlworkbench:*",
        "datazone:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:List*",
        "kms:Get*",
        "kms:Describe*",
        "kms:Decrypt",
```

```
        "kms:Encrypt",
        "kms:ReEncrypt*",
        "kms:Verify",
        "kms:Sign",
        "kms:GenerateDataKey",
        "glue:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/datazone:projectId" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchGet*",
        "glue:SearchTables",
        "glue:List*",
        "glue:Get*",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:PutResourcePolicy",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
```

```
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:UpdatePartition",
        "glue:NotifyEvent",
        "glue:DeleteResourcePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "NotAction" : [
        "s3:List*",
        "s3:Get*",
        "s3:Describe*",
        "s3:DeleteObjectVersion",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutObjectRetention",
        "s3:DeleteObject",
        "kms:List*",
        "kms:Get*",
        "kms:Describe*",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEncrypt*",
        "kms:Verify",
        "kms:Sign",
        "kms:GenerateDataKey",
        "ec2:Describe*",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "logs:*",
        "athena:*",
        "glue:BatchGet*",
        "glue:Get*",
        "glue:SearchTables",
        "glue:List*",
        "glue:CreateDatabase",
```

```
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:PutResourcePolicy",
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:UpdatePartition",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:StopCrawler",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:UpdateCrawler",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:StartCrawler",
        "glue:ResetJobBookmark",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:StopCrawlerSchedule",
        "glue:ResumeWorkflowRun",
        "glue:DeleteCrawler",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:UpdateCrawlerSchedule",
        "glue:DeleteConnection",
        "glue:UpdateConnection",
        "glue:BatchDeleteConnection",
        "glue:StartCrawlerSchedule",
```

```
        "glue:StartJobRun",
        "glue:CreateWorkflow",
        "glue:*DataQuality*",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:DeleteResourcePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "lakeformation:GetDataAccess",
        "lakeformation:BatchGrantPermissions",
        "lakeformation:GrantPermissions",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "ram:*",
        "redshift:*",
        "redshift-data:*",
        "tag:GetResources",
        "iam:List*",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:PassRole",
        "sqlworkbench:*",
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDataZoneRedshiftGlueProvisioningPolicy

Deskripsi: Amazon DataZone adalah layanan manajemen data yang memungkinkan Anda membuat katalog, menemukan, mengatur, berbagi, dan menganalisis data Anda. Dengan Amazon DataZone, Anda dapat berbagi dan mengakses data di seluruh akun dan wilayah yang didukung. Amazon DataZone menyederhanakan pengalaman Anda di seluruh AWS layanan, termasuk, namun tidak terbatas pada, Amazon Redshift, Amazon Athena, Glue, AWS dan AWS Lake Formation.

`AmazonDataZoneRedshiftGlueProvisioningPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneRedshiftGlueProvisioningPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 September 2023, 20:19 UTC
- Waktu teredit: 21 Agustus 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZonePermissionsToCreateEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/datazone*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonDataZoneEnvironmentRolePermissionsBoundary",
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ],
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToManageCreatedEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:GetRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneCFStackCreationForEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneCFStackManagementForEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentParameterValidation",
```

```
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:ListPermissions",
        "glue:CreateDatabase",
        "glue:GetDatabase",
        "athena:GetWorkGroup",
        "logs:DescribeLogGroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift:DescribeClusters",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:ListResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentGlueDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteDatabase"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentAthenaDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteWorkGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentAthenaResourceCreation",
      "Effect" : "Allow",
      "Action" : [
        "athena:CreateWorkGroup",
        "athena:TagResource",
        "iam:TagRole",
        "iam:TagPolicy",
        "logs:TagLogGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentLogGroupCreation",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:datazone-*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentLogGroupManagement",
      "Action" : [
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:datazone-*",
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentIAMPolicyManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeletePolicy",
```

```
        "iam:CreatePolicy",
        "iam:GetPolicy",
        "iam:ListPolicyVersions",
        "iam:DeletePolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentS3ValidationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentKMSDecryptPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToTagAmazonDataZoneEnvironmentGlueResources",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToGetAmazonDataZoneEnvironmentBlueprintTemplates",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "RedshiftDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ListSchemas",
        "redshift-data:ExecuteStatement"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "DescribeStatementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetSecretValuePermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDataZoneRedshiftManageAccessRolePolicy

Deskripsi: Kebijakan ini memberikan DataZone izin kepada Amazon untuk menerbitkan data Amazon Redshift ke katalog. Ini juga memberikan DataZone izin Amazon untuk memberikan akses atau mencabut akses ke aset yang diterbitkan Amazon Redshift atau Amazon Redshift Serverless dalam katalog.

`AmazonDataZoneRedshiftManageAccessRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneRedshiftManageAccessRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 September 2023, 20:15 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "redshiftDataScopeDownPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:ListTables",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift:*:*:cluster:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "listSecretsPermission",
      "Effect" : "Allow",
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*"
    },
    {
      "Sid" : "getWorkgroupPermission",
      "Effect" : "Allow",
      "Action" : "redshift-serverless:GetWorkgroup",
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "createAndDeleteWorkgroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateWorkgroup",
        "redshift-serverless:DeleteWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "getNamespacePermission",
      "Effect" : "Allow",
      "Action" : "redshift-serverless:GetNamespace",
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "createAndDeleteNamespacePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateNamespace",
        "redshift-serverless:DeleteNamespace"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "redshiftDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift:DescribeClusters"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "dataSharesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare",
        "redshift:DescribeDataShares"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:datashare:*/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "associateDataShareConsumerPermission",
      "Effect" : "Allow",
      "Action" : "redshift:AssociateDataShareConsumer",
      "Resource" : "arn:aws:redshift:*:*:datashare:*/datazone*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

Deskripsi: AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary Kebijakan adalah daftar izin yang diizinkan pada peran eksekusi yang dibuat di SageMaker lingkungan yang disediakan oleh Amazon DataZone.

`AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 April 2024, 23:01 UTC
- Waktu teredit: 17 Juli 2026, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`

Versi kebijakan

Versi kebijakan: v13 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
```

```
      ]
    },
    {
      "Sid" : "AllowSageMakerProfileManagement",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DescribeUserProfile",
        "sagemaker:UpdateUserProfile",
        "sagemaker:CreatePresignedDomainUrl"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:*/*"
    },
    {
      "Sid" : "AllowLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAddTagsForDomainResources",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:user-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : [
            "CreateApp",
            "CreateSpace",
            "CreateUserProfile"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStudioActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListApps",
        "sagemaker:ListDomains",
        "sagemaker:ListSpaces",
        "sagemaker:ListUserProfiles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppActionsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*/*/*/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAppActionsForSharedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Shared"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "AllowMutatingActionsOnSharedSpacesWithoutOwner",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:UpdateSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:UpdateSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private",
            "Shared"
          ]
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
```

```
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowFlowDefinitionActions",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceActions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:*",
        "datazone:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
```

```
        "application-autoscaling:RegisterScalableTarget",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:StartImageScan",
        "elastic-inference:Connect",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "groundtruthlabeling:*",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
```

```
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:UpdateLogDelivery",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-serverless:GetCredentials",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "secretsmanager:ListSecrets",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "sns:ListTopics",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowRAMInvitation",
      "Effect" : "Allow",
      "Action" : "ram:AcceptResourceShareInvitation",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : "dzd*"
        }
      }
    },
```

```
    {
      "Sid" : "AllowECRActions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
        "ecr:PutImage",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker*",
        "arn:aws:ecr:*:*:repository/datazone*"
      ]
    },
    {
      "Sid" : "AllowCodeCommitActions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:*sagemaker*",
        "arn:aws:codecommit:*:*:*SageMaker*",
        "arn:aws:codecommit:*:*:*Sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeBuildActions",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker*",
        "arn:aws:codebuild:*:*:build/*"
```

```
      ]
    },
    {
      "Sid" : "AllowStepFunctionsActions",
      "Effect" : "Allow",
      "Action" : [
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:statemachine:*sagemaker*",
        "arn:aws:states:*:*:execution:*sagemaker*:*"
      ]
    },
    {
      "Sid" : "AllowSecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
    {
      "Sid" : "AllowServiceCatalogProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ProvisionProduct"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::Sagemaker-DataZone*",
        "arn:aws:s3:::DataZone-Sagemaker*",
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::amazon-datazone*"
      ]
    },
    {
      "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
```

```
          "s3:ExistingObjectTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors"
      ],
      "Resource" : [
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::Sagemaker-DataZone*",
        "arn:aws:s3:::DataZone-Sagemaker*",
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::amazon-datazone*"
      ]
    },
    {
      "Sid" : "ReadSageMakerJumpstartArtifacts",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
```

```
        "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
      ]
    },
    {
      "Sid" : "AllowLambdaInvokeFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSNSActions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish"
```

```
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForSageMakerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr_sagemaker_execution_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "bedrock.amazonaws.com",
            "states.amazonaws.com",
            "lakeformation.amazonaws.com",
            "events.amazonaws.com",
            "sagemaker.amazonaws.com",
            "forecast.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountKmsOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "KmsOperationsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:RetireGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AllowAthenaActions",
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
```

```
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowGlueCreateDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default"
      ]
    },
    {
      "Sid" : "AllowRedshiftGetClusterCredentials",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
```

```
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowListTags",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:domain/*"
      ]
    },
    {
      "Sid" : "AllowCloudformationListStackResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:ListJobs",
        "glue:CreateSession",
        "glue:RunStatement",
        "glue:BatchCreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:BatchGetWorkflows",
        "glue:BatchUpdatePartition",
        "glue:BatchDeletePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:UpdateTable",
        "glue:DeleteTableVersion",
        "glue:DeleteTable",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
```

```
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchDeleteTable",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:UpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDataQualityRuleset",
        "glue:CreateWorkflow",
        "glue:GetDatabases",
        "glue:GetTables",
        "glue:GetTable",
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:ListSchemas",
        "glue:BatchGetJobs",
        "glue:GetConnection",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowGlueActionsWithEnvironmentTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:StopCrawler",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:UpdateCrawler",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:StartCrawler",
        "glue:ResetJobBookmark",
```

```
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:StopCrawlerSchedule",
        "glue:ResumeWorkflowRun",
        "glue:ListSchemas",
        "glue:DeleteCrawler",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:UpdateCrawlerSchedule",
        "glue:DeleteConnection",
        "glue:UpdateConnection",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetTable",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchDeleteConnection",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:CreateWorkflow",
        "glue:*DataQuality*"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGlueDefaultAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchGet*",
        "glue:Get*",
        "glue:SearchTables",
        "glue:List*",
        "glue:RunStatement"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
```

```
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:connection/dz-sm-*",
        "arn:aws:glue:*:*:session/*"
      ]
    },
    {
      "Sid" : "AllowRedshiftClusterActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowCreateClusterUser",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateClusterUser"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*"
      ]
    },
    {
      "Sid" : "AllowCreateSecretActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "false",
```

```
          "aws:RequestTag/AmazonDataZoneProject" : "false",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false",
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "ForecastOperations",
      "Effect" : "Allow",
      "Action" : [
        "forecast:CreateExplainabilityExport",
        "forecast:CreateExplainability",
        "forecast:CreateForecastEndpoint",
        "forecast:CreateAutoPredictor",
        "forecast:CreateDatasetImportJob",
        "forecast:CreateDatasetGroup",
        "forecast:CreateDataset",
        "forecast:CreateForecast",
        "forecast:CreateForecastExportJob",
        "forecast:CreatePredictorBacktestExportJob",
        "forecast:CreatePredictor",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeExplainability",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeForecastEndpoint",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeDataset",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:GetAccuracyMetrics",
        "forecast:InvokeForecastEndpoint",
        "forecast:GetRecentForecastContext",
        "forecast:DescribePredictor",
        "forecast:TagResource",
        "forecast:DeleteResourceTree"
      ],
      "Resource" : [
        "arn:aws:forecast:*:*:*Canvas*"
```

```
      ]
    },
    {
      "Sid" : "RDSOperation",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEventBridgeRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeTagBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeListTagOperation",
      "Effect" : "Allow",
      "Action" : "events:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEMR",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSSOAction",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplicationAssignment",
        "sso:AssociateProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyNotAction",
      "Effect" : "Deny",
      "NotAction" : [
        "sagemaker:*",
        "sagemaker-geospatial:*",
        "sqlworkbench:*",
        "datazone:*",
        "forecast:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
```

```
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
```

```
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ListStackResources",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:CreateRepository",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
```

```
        "ecr:DeleteRepository",
        "ecr:PutImage",
        "ecr:StartImageScan",
        "ecr:TagResource",
        "ecr:UntagResource",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListClusters",
        "events:PutRule",
        "events:DescribeRule",
        "events:PutTargets",
        "events:TagResource",
        "events:ListTagsForResource",
        "fsx:DescribeFileSystems",
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:StopCrawler",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:UpdateCrawler",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:StartCrawler",
        "glue:ResetJobBookmark",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:StopCrawlerSchedule",
        "glue:ResumeWorkflowRun",
        "glue:DeleteCrawler",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:BatchGet*",
        "glue:UpdateCrawlerSchedule",
        "glue:DeleteConnection",
        "glue:UpdateConnection",
        "glue:Get*",
        "glue:BatchDeleteConnection",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
```

```
        "glue:CreateWorkflow",
        "glue:*DataQuality*",
        "glue:List*",
        "glue:CreateSession",
        "glue:RunStatement",
        "glue:BatchCreatePartition",
        "glue:CreateDatabase",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:BatchUpdatePartition",
        "glue:BatchDeletePartition",
        "glue:UpdateTable",
        "glue:DeleteTableVersion",
        "glue:DeleteTable",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchDeleteTable",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:UpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "groundtruthlabeling:*",
        "iam:CreateServiceLinkedRole",
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole",
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:RetireGrant",
        "lakeformation:GetDataAccess",
        "lambda:ListFunctions",
        "lambda:InvokeFunction",
        "logs:CreateLogDelivery",
```

```
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:UpdateLogDelivery",
        "ram:AcceptResourceShareInvitation",
        "rds:DescribeDBInstances",
        "redshift:CreateClusterUser",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:DescribeClusters",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "s3:GetBucketAcl",
        "s3:PutObjectAcl",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors",
        "s3:DeleteObjectVersion",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
```

```
        "secretsmanager:ListSecrets",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:TagResource",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:ProvisionProduct",
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish",
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine",
        "tag:GetResources",
        "sso:CreateApplicationAssignment",
        "sso:AssociateProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyUpdateNotebookInstanceLifecycleConfig",
      "Effect" : "Deny",
      "Action" : [
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDataZoneSageMakerManageAccessRolePolicy

Deskripsi: AmazonDataZoneSageMakerManageAccessRolePolicy Kebijakan ini memberi Amazon DataZone izin yang diperlukan untuk memberikan akses pengguna ke berbagai sumber daya di SageMaker lingkungan.

`AmazonDataZoneSageMakerManageAccessRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneSageMakerManageAccessRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 April 2024, 23:34 UTC
- Waktu teredit: 12 Februari 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerManageAccessRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:ListModelPackages",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:ListTags",
        "sagemaker:DescribeDomain",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:Search"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerTaggingPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:shared-with:*"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelPackageGroupPolicyPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:DeleteModelPackageGroupPolicy"
```

```
      ],
      "Resource" : [
        "arn:*:sagemaker:*:*:model-package-group/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerRAMPermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerRAMResourcePolicyPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:PutResourcePolicy",
        "sagemaker:GetResourcePolicy",
        "sagemaker:DeleteResourcePolicy"
      ],
      "Resource" : [
        "arn:*:sagemaker:*:*:feature-group/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerRAMTagResourceSharePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
      ],
      "Resource" : "arn:*:ram:*:*:resource-share/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AwsDataZoneDomainId" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerRAMDeleteResourceSharePermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ram:DeleteResourceShare"
      ],
      "Resource" : "arn:*:ram:*:*:resource-share/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AwsDataZoneDomainId" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerRAMCreateResourceSharePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:RequestedResourceType" : [
            "sagemaker:*"
          ]
        },
        "Null" : {
          "aws:RequestTag/AwsDataZoneDomainId" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerS3BucketPolicyPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::amazon-datazone*",
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
```

```
    {
      "Sid" : "AmazonSageMakerS3Permission",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::amazon-datazone*",
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerECRPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetRepositoryPolicy",
        "ecr:SetRepositoryPolicy",
        "ecr:DeleteRepositoryPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerKMSReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AmazonSageMakerKMSGrantPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDataZoneSageMakerProvisioningRolePolicy

Deskripsi: AmazonDataZoneSageMakerProvisioningRolePolicy Kebijakan ini memberi Amazon izin DataZone yang diperlukan untuk bekerja sama dengan Amazon SageMaker.

`AmazonDataZoneSageMakerProvisioningRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneSageMakerProvisioningRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 April 2024, 23:32 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerProvisioningRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSageMakerStudio",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateDomain"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
```

```
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false",
          "aws:RequestTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteSageMakerStudio",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteDomain"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentSageMakerDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "sagemaker.amazonaws.com"
          ],
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToCreateEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ],
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary"
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToManageEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToCreateSageMakerServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentParameterValidation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "sagemaker:ListDomains"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentKMSKeyValidation",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentGluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection",
        "glue:DeleteConnection",
        "glue:GetConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/dz-sm-athena-glue-connection-*",
        "arn:aws:glue:*:*:connection/dz-sm-redshift-cluster-connection-*",
        "arn:aws:glue:*:*:connection/dz-sm-redshift-serverless-connection-*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
```

```
            "cloudformation.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDetectiveFullAccess

Deskripsi: Menyediakan akses penuh ke layanan Amazon Detective dan akses cakupan ke dependensi UI konsol

`AmazonDetectiveFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDetectiveFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 April 2020, 17:57 UTC
- Waktu teredit: 17 Mei 2023, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "detective:*",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:ArchiveFindings"
      ],
      "Resource" : "arn:aws:guardduty:*:*:detector/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "securityHub:GetFindings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDetectiveInvestigatorAccess

Deskripsi: Menyediakan akses penyelidik ke layanan Amazon Detective dan akses cakupan ke dependensi UI konsol. Kebijakan ini memberikan izin untuk menyelami Detektif untuk tujuan investigasi dan akses menulis terbatas ke Guardduty.

`AmazonDetectiveInvestigatorAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDetectiveInvestigatorAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Januari 2023, 15:24 UTC
- Waktu teredit: 27 November 2023, 03:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DetectivePermissions",
      "Effect" : "Allow",
      "Action" : [
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:DescribeOrganizationConfiguration",
        "detective:GetFreeTrialEligibility",
        "detective:GetGraphIngestState",
        "detective:GetMembers",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListDatasourcePackages",
        "detective:ListGraphs",
        "detective:ListHighDegreeEntities",
        "detective:ListInvitations",
        "detective:ListMembers",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "detective:SearchGraph",
        "detective:StartInvestigation",
        "detective:GetInvestigation",
        "detective:ListInvestigations",
        "detective:UpdateInvestigationState",
        "detective:ListIndicators",
        "detective:InvokeAssistant"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "GuardDutyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:ArchiveFindings",
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubPermissions",
      "Effect" : "Allow",
      "Action" : [
        "securityHub:GetFindings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDetectiveMemberAccess

Deskripsi: Menyediakan akses anggota ke layanan Amazon Detective dan akses cakupan ke dependensi UI konsol.

`AmazonDetectiveMemberAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDetectiveMemberAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Januari 2023, 15:16 UTC
- Waktu teredit: 17 Januari 2023, 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "detective:AcceptInvitation",
        "detective:BatchGetMembershipDatasources",
        "detective:DisassociateMembership",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations",
        "detective:RejectInvitation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDetectiveOrganizationsAccess

Deskripsi: Menyediakan akses Organisasi untuk mengelola administrator yang didelegasikan untuk Amazon Detective dan akses cakupan ke dependensi UI konsol. Ini juga memberikan izin untuk membuat peran terkait layanan untuk Detektif.

`AmazonDetectiveOrganizationsAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDetectiveOrganizationsAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Maret 2023, 15:20 UTC
- Waktu teredit: 02 Maret 2023, 15:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "detective:DisableOrganizationAdminAccount",
        "detective:EnableOrganizationAdminAccount",
        "detective:ListOrganizationAdminAccount"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "detective.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "detective.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "detective.amazonaws.com",
            "guardduty.amazonaws.com",
            "macie.amazonaws.com",
            "securityhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDetectiveServiceLinkedRolePolicy

Deskripsi: Memungkinkan Amazon Detective untuk melakukan panggilan layanan atas nama Anda

`AmazonDetectiveServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 18 November 2021, 19:47 UTC
- Waktu teredit: 18 November 2021, 19.47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDevOpsGuruConsoleFullAccess

Deskripsi: Kebijakan ini memberikan akses penuh ke konsol DevOps Guru.

`AmazonDevOpsGuruConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDevOpsGuruConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Desember 2021, 18:43 UTC
- Waktu teredit: 25 Agustus 2022 18.18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CloudFormationListStacksAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsListTopicsAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsTopicOperations",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:DevOps-Guru-*"
    },
    {
      "Sid" : "DevOpsGuruSlrCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "devops-guru.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "DevOpsGuruSlrDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
    },
    {
      "Sid" : "RDSDescribeDBInstancesAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PerformanceInsightsMetricsDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics",
        "pi:DescribeDimensionKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsFilterLogEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDevOpsGuruFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon DevOps Guru.

`AmazonDevOpsGuruFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDevOpsGuruFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2020, 16:38 UTC
- Waktu teredit: 25 Agustus 2022 18.23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationListStacksAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsListTopicsAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsTopicOperations",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "sns:Publish"
      ],
```

```
      "Resource" : "arn:aws:sns:*:*:DevOps-Guru-*"
    },
    {
      "Sid" : "DevOpsGuruSlrCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "devops-guru.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DevOpsGuruSlrDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
    },
    {
      "Sid" : "RDSDescribeDBInstancesAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsFilterLogEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDevOpsGuruOrganizationsAccess

Deskripsi: Menyediakan akses untuk mengaktifkan dan mengelola Amazon DevOps Guru dalam organisasi.

`AmazonDevOpsGuruOrganizationsAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDevOpsGuruOrganizationsAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 November 2021, 23:50 UTC
- Waktu teredit: 15 November 2021, 23:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:DescribeOrganizationHealth",
        "devops-guru:DescribeOrganizationResourceCollectionHealth",
        "devops-guru:DescribeOrganizationOverview",
        "devops-guru:ListOrganizationInsights",
        "devops-guru:SearchOrganizationInsights"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListRoots"
      ],
      "Resource" : "arn:aws:organizations::*:"
    },
    {
      "Sid" : "OrganizationsAdminDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "devops-guru.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDevOpsGuruReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon DevOps Guru Console.

`AmazonDevOpsGuruReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDevOpsGuruReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2020, 16:34 UTC
- Waktu teredit: 25 Agustus 2022 18.11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:DescribeAccountHealth",
        "devops-guru:DescribeAccountOverview",
        "devops-guru:DescribeAnomaly",
        "devops-guru:DescribeEventSourcesConfig",
        "devops-guru:DescribeFeedback",
        "devops-guru:DescribeInsight",
        "devops-guru:DescribeResourceCollectionHealth",
        "devops-guru:DescribeServiceIntegration",
        "devops-guru:GetCostEstimation",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListAnomaliesForInsight",
        "devops-guru:ListEvents",
        "devops-guru:ListInsights",
        "devops-guru:ListAnomalousLogGroups",
        "devops-guru:ListMonitoredResources",
        "devops-guru:ListNotificationChannels",
        "devops-guru:ListRecommendations",
        "devops-guru:SearchInsights",
        "devops-guru:StartCostEstimation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationListStacksAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSDescribeDBInstancesAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsFilterLogEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDevOpsGuruServiceRolePolicy

Deskripsi: Peran terkait layanan yang diperlukan agar Amazon dapat DevOpsGuru mengakses sumber daya Anda.

`AmazonDevOpsGuruServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 01 Desember 2020, 10:24 UTC
- Waktu teredit: 10 Januari 2023, 14:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "cloudtrail:LookupEvents",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:ListDashboards",
        "cloudwatch:GetDashboard",
        "cloudformation:GetTemplate",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListImports",
        "codedeploy:BatchGetDeployments",
        "codedeploy:GetDeploymentGroup",
        "codedeploy:ListDeployments",
        "config:DescribeConfigurationRecorderStatus",
        "config:GetResourceConfigHistory",
        "events:ListRuleNamesByTarget",
        "xray:GetServiceGraph",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "pi:GetResourceMetrics",
        "tag:GetResources",
        "lambda:GetFunction",
        "lambda:GetFunctionConcurrency",
        "lambda:GetAccountSettings",
        "lambda:ListProvisionedConcurrencyConfigs",
        "lambda:ListAliases",
        "lambda:ListEventSourceMappings",
        "lambda:GetPolicy",
        "ec2:DescribeSubnets",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
```

```
        "sqs:GetQueueAttributes",
        "kinesis:DescribeStream",
        "kinesis:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeStream",
        "dynamodb:ListStreams",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeAccountAttributes",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "s3:GetBucketNotification",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketWebsite",
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListStorageLensConfigurations",
        "servicequotas:GetServiceQuota",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListServiceQuotas"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPutTargetsOnASpecificRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/DevOps-Guru-managed-*"
    },
    {
```

```
      "Sid" : "AllowCreateOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAddTagsToOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
      "Sid" : "AllowAccessOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-GuruInsightSsmOpsItemRelated" : "true"
        }
      }
    },
    {
      "Sid" : "AllowCreateManagedRule",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
    },
    {
      "Sid" : "AllowAccessManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
    },
```

```
    {
      "Sid" : "AllowOtherOperationsOnManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "devops-guru.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowTagBasedFilterLogEvents",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAPIGatewayGetIntegrations",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/restapis/??????????",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDMSCloudWatchLogsRole

Deskripsi: Menyediakan akses untuk mengunggah log replikasi DMS ke log cloudwatch di akun pelanggan.

`AmazonDMSCloudWatchLogsRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDMSCloudWatchLogsRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 Januari 2016, 23:44 UTC
- Waktu teredit: 23 Mei 2023, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDescribeOnAllLogGroups",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeOfAllLogStreamsOnDmsTasksLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*"
      ]
    },
    {
      "Sid" : "AllowCreationOfDmsLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:"
      ]
    },
    {
      "Sid" : "AllowCreationOfDmsLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*:log-stream:dms-task-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:dms-
serverless-*"
      ]
    },
    {
      "Sid" : "AllowUploadOfLogEventsToDmsLogStream",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*:log-stream:dms-task-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:dms-
serverless-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDMSRedshiftS3Role

Deskripsi: Menyediakan akses untuk mengelola pengaturan S3 untuk titik akhir Redshift untuk DMS.

`AmazonDMSRedshiftS3Role`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDMSRedshiftS3Role` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 April 2016, 17:05 UTC
- Waktu teredit: 08 Juli 2019, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:DeleteBucket",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:GetBucketAcl",
        "s3:PutBucketVersioning",
        "s3:GetBucketVersioning",
        "s3:PutLifecycleConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:DeleteBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::dms-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDMSVPCManagementRole

Deskripsi: Menyediakan akses untuk mengelola setelan VPC untuk konfigurasi pelanggan AWS terkelola

`AmazonDMSVPCManagementRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDMSVPCManagementRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 18 November 2015, 16:33 UTC
- Waktu teredit: 25 Juli 2024, 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Statement1",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDocDB-ElasticServiceRolePolicy

Deskripsi: Mengiz DocumentDB-Elastic inkan Amazon mengelola AWS sumber daya atas nama Anda.

`AmazonDocDB-ElasticServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran

- Waktu pembuatan: 30 November 2022, 14:17 UTC
- Waktu teredit: 30 November 2022, 14:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB-Elastic"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDocDBConsoleFullAccess

Deskripsi: Menyediakan akses penuh untuk mengelola Amazon DocumentDB dengan kompatibilitas MongoDB menggunakan. Konsol Manajemen AWS Perhatikan bahwa kebijakan ini juga memberikan akses penuh untuk mempublikasikan semua topik SNS dalam akun, izin untuk membuat dan mengedit instans Amazon EC2 dan konfigurasi VPC, izin untuk melihat dan mencantumkan kunci di Amazon KMS, dan akses penuh ke Amazon RDS dan Amazon Neptune.

`AmazonDocDBConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDocDBConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Januari 2019, 20:37 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DocdbSids",
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:CreateCluster",
```

```
        "docdb-elastic:UpdateCluster",
        "docdb-elastic:GetCluster",
        "docdb-elastic:DeleteCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:CreateClusterSnapshot",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:DeleteClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:RestoreClusterFromSnapshot",
        "docdb-elastic:TagResource",
        "docdb-elastic:UntagResource",
        "docdb-elastic:ListTagsForResource",
        "docdb-elastic:CopyClusterSnapshot",
        "docdb-elastic:StartCluster",
        "docdb-elastic:StopCluster",
        "docdb-elastic:GetPendingMaintenanceAction",
        "docdb-elastic:ListPendingMaintenanceActions",
        "docdb-elastic:ApplyPendingMaintenanceAction",
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBInstance",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:CreateGlobalCluster",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DeleteGlobalCluster",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
```

```
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:ModifyGlobalCluster",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveFromGlobalCluster",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "DependencySids",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DocdbSLRSid",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DocdbElasticSLRSid",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/
AWSServiceRoleForDocDB-Elastic",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "docdb-elastic.amazonaws.com"
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDocDBElasticFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon DocumentDB Elastic Clusters dan izin lain yang diperlukan untuk dependensinya termasuk EC2, KMS, SecretsManager dan IAM. CloudWatch

`AmazonDocDBElasticFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDocDBElasticFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Juni 2023, 13:51 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DocdbElasticSid",
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:CreateCluster",
        "docdb-elastic:UpdateCluster",
        "docdb-elastic:GetCluster",
        "docdb-elastic:DeleteCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:CreateClusterSnapshot",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:DeleteClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:RestoreClusterFromSnapshot",
        "docdb-elastic:TagResource",
        "docdb-elastic:UntagResource",
        "docdb-elastic:ListTagsForResource",
        "docdb-elastic:CopyClusterSnapshot",
        "docdb-elastic:StartCluster",
        "docdb-elastic:StopCluster",
        "docdb-elastic:GetPendingMaintenanceAction",
        "docdb-elastic:ListPendingMaintenanceActions",
        "docdb-elastic:ApplyPendingMaintenanceAction"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2Sid",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints",
        "ec2:ModifyVpcEndpoint",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "docdb-elastic.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KMSSid",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "docdb-elastic.*.amazonaws.com"
          ],
          "aws:ResourceTag/DocDBElasticFullAccess" : "*"
        }
      }
    },
    {
      "Sid" : "KMSGrantSid",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/DocDBElasticFullAccess" : "*",
          "kms:ViaService" : [
            "docdb-elastic.*.amazonaws.com"
```

```
          ]
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Sid" : "SecretManagerSid",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:GetResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/DocDBElasticFullAccess" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "docdb-elastic.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudwatchSid",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SLRSid",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/
AWSServiceRoleForDocDB-Elastic",
```

```
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "docdb-elastic.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDocDBElasticReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke Amazon DocDB-Elastic dan CloudWatch metrik.

`AmazonDocDBElasticReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDocDBElasticReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Juni 2023, 14:37 UTC
- Waktu teredit: 21 Juni 2023, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:ListClusters",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDocDBFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon DocumentDB dengan kompatibilitas MongoDB. Perhatikan bahwa kebijakan ini juga memberikan akses penuh untuk mempublikasikan semua topik SNS dalam akun dan akses penuh ke Amazon RDS dan Amazon Neptune.

`AmazonDocDBFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDocDBFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Januari 2019, 20:21 UTC
- Waktu teredit: 09 Januari 2019, 20:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
```

```
        "rds:CopyDBParameterGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBInstance",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
```

```
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDocDBReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke Amazon DocumentDB dengan kompatibilitas MongoDB. Perhatikan bahwa kebijakan ini juga memberikan akses ke sumber daya Amazon RDS dan Amazon Neptune.

`AmazonDocDBReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDocDBReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Januari 2019, 20:30 UTC
- Waktu teredit: 09 Januari 2019, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "kms:ListAliases",
        "kms:ListKeyPolicies"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/docdb/*:log-stream:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDRSVPCManajemen

Deskripsi: Menyediakan akses untuk mengelola pengaturan VPC untuk konfigurasi pelanggan yang dikelola Amazon

`AmazonDRSVPCManagement`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDRSVPCManagement` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 September 2015, 00:09 UTC
- Waktu teredit: 02 September 2015, 00:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDRSVPCManagement`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDynamoDBFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon DynamoDB melalui. Konsol Manajemen AWS

`AmazonDynamoDBFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDynamoDBFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 29 Januari 2021, 17:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "dynamodb:*",
        "dax:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:GetMetricData",
        "datapipeline:ActivatePipeline",
```

```
        "datapipeline:CreatePipeline",
        "datapipeline:DeletePipeline",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:PutPipelineDefinition",
        "datapipeline:QueryObjects",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes",
        "lambda:CreateFunction",
        "lambda:ListFunctions",
        "lambda:ListEventSourceMappings",
        "lambda:CreateEventSourceMapping",
        "lambda:DeleteEventSourceMapping",
        "lambda:GetFunctionConfiguration",
        "lambda:DeleteFunction",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupQuery",
        "resource-groups:DeleteGroup",
        "resource-groups:CreateGroup",
        "tag:GetResources",
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
```

```
    {
      "Action" : "cloudwatch:GetInsightRuleReport",
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com",
            "application-autoscaling.amazonaws.com.cn",
            "dax.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "replication.dynamodb.amazonaws.com",
            "dax.amazonaws.com",
            "dynamodb.application-autoscaling.amazonaws.com",
            "contributorinsights.dynamodb.amazonaws.com",
            "kinesisreplication.dynamodb.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDynamoDBFullAccess_v2

Deskripsi: Menyediakan akses penuh ke Amazon DynamoDB

`AmazonDynamoDBFullAccess_v2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDynamoDBFullAccess_v2` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 Mei 2025, 14:52 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess_v2`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "DDBAndDAXFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:*",
        "dax:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSIntegration",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaIntegration",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DaxSNSIntegration",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingIntegration",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "dynamodb"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagManagement",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchMonitoring",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListKinesisResources",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ListEC2ResourcesForDaxClusterCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchInsightsRules",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetInsightRuleReport",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    },
    {
      "Sid" : "ServiceRoleCreation",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "replication.dynamodb.amazonaws.com",
            "dax.amazonaws.com",
            "dynamodb.application-autoscaling.amazonaws.com",
            "contributorinsights.dynamodb.amazonaws.com",
            "kinesisreplication.dynamodb.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamIntegration",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDynamoDBFullAccesswithDataPipeline

Deskripsi: Kebijakan ini berada di jalur penghentian. Lihat dokumentasi untuk panduan: Men https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DynamoDBPipeline.html. yediakan akses penuh ke Amazon DynamoDB termasuk Export/Import menggunakan Pipeline AWS Data melalui. Konsol Manajemen AWS

`AmazonDynamoDBFullAccesswithDataPipeline`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDynamoDBFullAccesswithDataPipeline` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 12 November 2015, 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "dynamodb:*",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "DDBConsole"
    },
    {
      "Action" : [
        "lambda:*",
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "DDBConsoleTriggers"
    },
    {
      "Action" : [
```

```
        "datapipeline:*",
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "DDBConsoleImportExport"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRolePolicy",
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Sid" : "IAMEDPRoles"
    },
    {
      "Action" : [
        "ec2:CreateTags",
        "ec2:DescribeInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "elasticmapreduce:*",
        "datapipeline:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "EMR"
    },
    {
      "Action" : [
        "s3:DeleteObject",
        "s3:Get*",
        "s3:List*",
        "s3:Put*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
```

```
      "Sid" : "S3"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonDynamoDBReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon DynamoDB melalui. Konsol Manajemen AWS

`AmazonDynamoDBReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDynamoDBReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 18 November 2024, 17:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralReadOnlyAccess",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "dynamodb:BatchGetItem",
        "dynamodb:Describe*",
        "dynamodb:List*",
        "dynamodb:GetAbacStatus",
        "dynamodb:GetItem",
        "dynamodb:GetResourcePolicy",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dax:Describe*",
        "dax:List*",
        "dax:GetItem",
        "dax:BatchGetItem",
        "dax:Query",
        "dax:Scan",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
```

```
        "kms:ListAliases",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "lambda:ListFunctions",
        "lambda:ListEventSourceMappings",
        "lambda:GetFunctionConfiguration",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupQuery",
        "tag:GetResources",
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CCIAccess",
      "Action" : "cloudwatch:GetInsightRuleReport",
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEBSCSIDriverEKSClusterScopedPolicy

Deskripsi: Kebijakan IAM yang memungkinkan akun layanan pengemudi CSI melakukan panggilan ke layanan terkait seperti EC2 atas nama Anda. Kebijakan ini membatasi driver Amazon EBS CSI untuk hanya mengelola volume EBS dan snapshot yang termasuk dalam cluster EKS tertentu. Ini membutuhkan tag sumber daya ebs.csi.aws. com/cluster-name untuk mencocokkan tag eks-cluster-

name pada prinsip IAM, mencegah akses lintas cluster ketika beberapa cluster berbagi yang sama. Akun AWS Operasi lampirkan dan lepaskan pada instance dibatasi untuk instance yang ditandai dengan tag eks: cluster-name (ditetapkan secara otomatis oleh EKS pada grup node terkelola) atau ebs.csi.aws. com/cluster-tag nama (untuk contoh yang ditandai secara manual).

`AmazonEBSCSIDriverEKSClusterScopedPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEBSCSIDriverEKSClusterScopedPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 April 2026, 17:27 UTC
- Waktu teredit: 28 Mei 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEBSCSIDriverEKSClusterScopedPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyDescribeOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSnapshots",
```

```
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVolumeStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateAndCopyVolumesWithClusterTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "CopyClusterVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/vol-*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsWithClusterTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsFromClusterVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "ManageClusterVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolume",
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "CreateVolumesFromAndEnableFSROnClusterSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "AttachDetachVolumesToClusterInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/eks:cluster-name" : "${aws:PrincipalTag/eks-cluster-name}"
        }
      }
    },
    {
      "Sid" : "AttachDetachVolumesToEKSStandardTaggedInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks-cluster-
name}"
        }
      }
    },
    {
      "Sid" : "AttachDetachVolumesToManuallyTaggedInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "DeleteAndLockClusterSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:LockSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "TagResourcesOnCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot",
            "CopyVolumes"
          ]
        }
      }
    },
    {
      "Sid" : "ModifyTagsOnClusterVolumes",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringNotEquals" : {
          "aws:TagKeys" : [
            "ebs.csi.aws.com/cluster",
            "ebs.csi.aws.com/cluster-name",
            "kubernetes.io/created-for/pvc/name"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEBSCSIDriverPolicy

Deskripsi: Kebijakan IAM yang memungkinkan akun layanan pengemudi CSI melakukan panggilan ke layanan terkait seperti EC2 atas nama Anda.

`AmazonEBSCSIDriverPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEBSCSIDriverPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 04 April 2022, 17:24 UTC
- Waktu teredit: 13 Mei 2026, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVolumeStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyVolumes"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/vol-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot",
            "CopyVolumes"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/CSIVolumeName" : "*"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/CSIVolumeName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/kubernetes.io/created-for/pvc/name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
```

```
        "StringLike" : {
          "aws:RequestTag/CSIVolumeSnapshotName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:LockSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/CSIVolumeSnapshotName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:LockSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEBSCSIDriverPolicyV2

Deskripsi: Kebijakan IAM yang memungkinkan akun layanan pengemudi EBS CSI melakukan panggilan ke layanan terkait seperti EC2 atas nama Anda. Ini membatasi driver Amazon EBS CSI untuk hanya mengelola volume EBS dan snapshot yang ditandai dengan kunci ebs.csi.aws. com/ cluster diatur ke true. Volume yang disediakan oleh plugin volume Kubernetes dalam pohon (CSI-migrated volume) juga didukung melalui kubernetes. io/created- for/pvc /tag sumber daya nama.

`AmazonEBSCSIDriverPolicyV2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEBSCSIDriverPolicyV2` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 April 2026, 17:27 UTC
- Waktu teredit: 16 April 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEBSCSIDriverPolicyV2`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyDescribeOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVolumeStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateAndCopyVolumesWithManagedTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Sid" : "CopyManagedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/vol-*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "CopyCSIMigratedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/vol-*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/kubernetes.io/created-for/pvc/name" : "*"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsWithManagedTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsFromManagedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Sid" : "ManageManagedVolumes",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolume",
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Sid" : "ManageCSIMigratedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolume",
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/kubernetes.io/created-for/pvc/name" : "*"
        }
      }
    },
    {
      "Sid" : "CreateVolumesFromAndEnableFSROnManagedSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "AttachDetachVolumesToAnyInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DeleteAndLockManagedSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:LockSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Sid" : "TagResourcesOnCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot",
            "CopyVolumes"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "ModifyTagsOnManagedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringNotEquals" : {
          "aws:TagKeys" : [
            "ebs.csi.aws.com/cluster",
            "ebs.csi.aws.com/cluster-name",
            "kubernetes.io/created-for/pvc/name"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEC2ContainerRegistryFullAccess

Deskripsi: Menyediakan akses administratif ke sumber daya Amazon ECR

`AmazonEC2ContainerRegistryFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2ContainerRegistryFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Desember 2015, 17:06 UTC
- Waktu teredit: 05 Desember 2020, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:*",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "replication.ecr.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEC2ContainerRegistryPowerUser

Deskripsi: Menyediakan akses penuh ke repositori Amazon EC2 Container Registry, tetapi tidak mengizinkan penghapusan repositori atau perubahan kebijakan.

`AmazonEC2ContainerRegistryPowerUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2ContainerRegistryPowerUser` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Desember 2015, 17:05 UTC
- Waktu teredit: 10 Desember 2019, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:GetLifecyclePolicy",
        "ecr:GetLifecyclePolicyPreview",
        "ecr:ListTagsForResource",
        "ecr:DescribeImageScanFindings",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:PutImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEC2ContainerRegistryPullOnly

Deskripsi: Menyediakan akses untuk menarik gambar dari repositori Amazon EC2 Container Registry.

`AmazonEC2ContainerRegistryPullOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2ContainerRegistryPullOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Oktober 2024, 16:58 UTC
- Waktu teredit: 04 Oktober 2024, 16:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPullOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchImportUpstreamImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEC2ContainerRegistryReadOnly

Deskripsi: Menyediakan akses baca-saja ke repositori Amazon EC2 Container Registry.

`AmazonEC2ContainerRegistryReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2ContainerRegistryReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Desember 2015, 17:04 UTC
- Waktu teredit: 10 Desember 2019, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:GetLifecyclePolicy",
        "ecr:GetLifecyclePolicyPreview",
        "ecr:ListTagsForResource",
        "ecr:DescribeImageScanFindings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEC2ContainerServiceAutoscaleRole

Deskripsi: Kebijakan untuk mengaktifkan Penskalaan Otomatis Tugas untuk Layanan Kontainer Amazon EC2

`AmazonEC2ContainerServiceAutoscaleRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2ContainerServiceAutoscaleRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 12 Mei 2016, 23:25 UTC
- Waktu teredit: 05 Februari 2018, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEC2ContainerServiceEventsRole

Deskripsi: Kebijakan untuk mengaktifkan A CloudWatch cara untuk Layanan Kontainer EC2

`AmazonEC2ContainerServiceEventsRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2ContainerServiceEventsRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 30 Mei 2017, 16:51 UTC
- Waktu teredit: 06 Maret 2023, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:RunTask"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ecs-tasks.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "ecs:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "RunTask"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEC2ContainerServiceforEC2Role

Deskripsi: Kebijakan default untuk Peran Amazon EC2 untuk Layanan Kontainer Amazon EC2.

`AmazonEC2ContainerServiceforEC2Role`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2ContainerServiceforEC2Role` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Maret 2015, 18:45 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags",
        "ecs:CreateCluster",
        "ecs:DeregisterContainerInstance",
        "ecs:DiscoverPollEndpoint",
        "ecs:Poll",
        "ecs:RegisterContainerInstance",
        "ecs:StartTelemetrySession",
        "ecs:UpdateContainerInstancesState",
        "ecs:Submit*",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterContainerInstance"
```

```
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task/*/*",
        "arn:aws:ecs:*:*:container-instance/*/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEC2ContainerServiceRole

Deskripsi: Kebijakan default untuk peran layanan Amazon ECS.

`AmazonEC2ContainerServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2ContainerServiceRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 09 April 2015, 16:14 UTC

- Waktu teredit: 11 Agustus 2016, 13:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:Describe*",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEC2FullAccess

Deskripsi: Menyediakan akses penuh ke Amazon EC2 melalui. Konsol Manajemen AWS

`AmazonEC2FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2FullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 27 November 2018, 02:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2FullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "ec2:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:*",
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "ec2scheduled.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "transitgateway.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEC2ImageReferencesAccessPolicy

Deskripsi: Menyediakan akses baca-saja untuk memindai semua jenis sumber daya yang didukung untuk data yang relevan saat menggunakan. DescribeImageReferences

`AmazonEC2ImageReferencesAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2ImageReferencesAccessPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Agustus 2025, 19:19 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ImageReferencesAccessPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:DescribeImageReferences",
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ssm:DescribeParameters",
        "ssm:GetParameters",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:GetContainerRecipe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ec2-images.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEC2ReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon EC2 melalui. Konsol Manajemen AWS

`AmazonEC2ReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 12 Februari 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:Describe*"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEC2RoleforAWSCodeDeploy

Deskripsi: Menyediakan akses EC2 ke bucket S3 untuk mengunduh revisi. Peran ini diperlukan oleh CodeDeploy agen pada instans EC2.

`AmazonEC2RoleforAWSCodeDeploy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2RoleforAWSCodeDeploy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Mei 2015, 18:10 UTC
- Waktu teredit: 20 Maret 2017, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEC2RoleforAWSCodeDeployLimited

Deskripsi: Menyediakan akses terbatas EC2 ke bucket S3 untuk mengunduh revisi. Peran ini diperlukan oleh CodeDeploy agen pada instans EC2.

`AmazonEC2RoleforAWSCodeDeployLimited`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2RoleforAWSCodeDeployLimited` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 24 Agustus 2020, 17:55 UTC
- Waktu teredit: 20 Januari 2022, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*/CodeDeploy/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
```

```
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEC2RoleforDataPipelineRole

Deskripsi: Kebijakan default untuk peran layanan Amazon EC2 Peran untuk Pipeline Data.

`AmazonEC2RoleforDataPipelineRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2RoleforDataPipelineRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 22 Februari 2016, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:*",
        "datapipeline:*",
        "dynamodb:*",
        "ec2:Describe*",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:ListInstance*",
        "elasticmapreduce:ModifyInstanceGroups",
        "rds:Describe*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "s3:*",
        "sdb:*",
        "sns:*",
        "sqs:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEC2RoleForSSM

Deskripsi: Kebijakan ini akan segera tidak digunakan lagi. Harap gunakan AmazonSSMManagedInstanceCore kebijakan untuk mengaktifkan fungsionalitas inti layanan Manajer AWS Sistem pada instans EC2. Untuk informasi lebih lanjut lihat https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-instance-profile.html

`AmazonEC2RoleforSSM`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2RoleforSSM` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 29 Mei 2015, 17:48 UTC
- Waktu teredit: 24 Januari 2019, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetEncryptionConfiguration",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEC2RolePolicyForLaunchWizard

Deskripsi: Kebijakan terkelola untuk peran LaunchWizard layanan Amazon untuk EC2

`AmazonEC2RolePolicyForLaunchWizard`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2RolePolicyForLaunchWizard` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 November 2019, 08:05 UTC
- Waktu teredit: 18 Agustus 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardResourceGroupID" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceRoute"
      ],
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardApplicationType" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:AssociateAddress",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeRegions",
```

```
        "ec2:DescribeVolumes",
        "ec2:DescribeRouteTables",
        "ec2:ModifyInstanceAttribute",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricData",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "LaunchWizardResourceGroupID",
            "LaunchWizardApplicationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/LaunchWizardResourceGroupID" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVolume"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardResourceGroupID" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectTagging",
        "s3:GetBucketLocation",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*",
        "arn:aws:s3:::launchwizard*",
        "arn:aws:s3:::aws-sap-data-provider/config.properties"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:Create*",
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "cloudformation:DescribeStackResources",
        "cloudformation:SignalResource",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "LaunchWizardResourceGroupID"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchGetItem",
        "dynamodb:PutItem",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "dynamodb:Scan",
        "s3:ListBucket",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:DeleteTable",
        "dynamodb:CreateTable",
        "s3:GetObject",
        "dynamodb:DescribeTable",
        "s3:GetBucketLocation",
        "dynamodb:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:s3:::launchwizard*",
        "arn:aws:dynamodb:*:*:table/LaunchWizard*",
        "arn:aws:sqs:*:*:LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/LaunchWizardApplicationType" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
```

```
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSSAP-InstallBackint",
        "arn:aws:ssm:*:*:document/AWSSAP-InstallBackintForAWSBackup"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:ListTagsForResource",
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "LaunchWizard*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEC2SpotFleetAutoscaleRole

Deskripsi: Kebijakan untuk mengaktifkan Penskalaan Otomatis untuk Amazon EC2 Spot Fleet

`AmazonEC2SpotFleetAutoscaleRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2SpotFleetAutoscaleRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Agustus 2016, 18:27 UTC
- Waktu teredit: 18 Februari 2019, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
```

```
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ec2.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ec2.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEC2SpotFleetTaggingRole

Deskripsi: Mengizinkan EC2 Spot Fleet meminta, menghentikan, dan menandai Instans Spot atas nama Anda.

`AmazonEC2SpotFleetTaggingRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2SpotFleetTaggingRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 29 Juni 2017, 18:19 UTC
- Waktu teredit: 23 April 2020, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:CreateTags",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      },
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:*/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonECS_ FullAccess

Deskripsi: Menyediakan akses administratif ke sumber daya Amazon ECS dan mengaktifkan fitur ECS melalui akses ke sumber daya AWS layanan lainnya, termasuk VPC, grup Penskalaan Otomatis, dan tumpukan. CloudFormation

`AmazonECS_FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonECS_FullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 November 2017, 21:36 UTC
- Waktu teredit: 02 September 2026, 14:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECS_FullAccess`

Versi kebijakan

Versi kebijakan: v22 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSIntegrationsManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
```

```
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:ListMeshes",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:Describe*",
        "autoscaling:UpdateAutoScalingGroup",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStack*",
        "cloudformation:UpdateStack",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "codedeploy:BatchGetApplicationRevisions",
        "codedeploy:BatchGetApplications",
        "codedeploy:BatchGetDeploymentGroups",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ContinueDeployment",
        "codedeploy:CreateApplication",
        "codedeploy:CreateDeployment",
        "codedeploy:CreateDeploymentGroup",
        "codedeploy:GetApplication",
        "codedeploy:GetApplicationRevision",
        "codedeploy:GetDeployment",
        "codedeploy:GetDeploymentConfig",
        "codedeploy:GetDeploymentGroup",
        "codedeploy:GetDeploymentTarget",
        "codedeploy:ListApplicationRevisions",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentConfigs",
        "codedeploy:ListDeploymentGroups",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "codedeploy:RegisterApplicationRevision",
        "codedeploy:StopDeployment",
```

```
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CancelSpotFleetRequests",
        "ec2:CreateInternetGateway",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteSubnet",
        "ec2:DeleteVpc",
        "ec2:Describe*",
        "ec2:DetachInternetGateway",
        "ec2:DisassociateRouteTable",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RequestSpotFleet",
        "ec2:RunInstances",
        "ecs:*",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateRule",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteRule",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget",
        "events:ListTargetsByRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "fsx:DescribeFileSystems",
```

```
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRoles",
        "lambda:ListFunctions",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:FilterLogEvents",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "servicediscovery:CreatePrivateDnsNamespace",
        "servicediscovery:CreateService",
        "servicediscovery:DeleteService",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetOperation",
        "servicediscovery:GetService",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:UpdateService",
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/aws/service/ecs*"
    },
    {
      "Sid" : "ManagedCloudformationResourcesCleanupPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteInternetGateway",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
```

```
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-name" : "EC2ContainerService-*"
        }
      }
    },
    {
      "Sid" : "TasksPassRolePolicy",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ecs-tasks.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InfrastructurePassRolePolicy",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsInfrastructureRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InstancePassRolePolicy",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsInstanceRole*"
      ],
```

```
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "AutoScalingPassRolePolicy",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsAutoscaleRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com",
            "application-autoscaling.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "ServiceLinkedRoleCreationPolicy",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "ecs.amazonaws.com",
            "autoscaling.amazonaws.com",
            "ecs.application-autoscaling.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ELBTaggingPolicy",
```

```
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateTargetGroup",
            "CreateRule",
            "CreateListener",
            "CreateLoadBalancer"
          ]
        }
      }
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack",
            "UpdateStack"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonECSComputeServiceRolePolicy

Deskripsi: Kebijakan untuk mengaktifkan Amazon ECS Compute untuk mengelola instans EC2 dan sumber daya terkait sebagai bagian dari instans terkelola ECS

`AmazonECSComputeServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 24 Maret 2025, 17:37 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSComputeServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyPermissionsForInstanceManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeFleets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyPermissionsForInstanceEventWindows",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceEventWindows"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyPermissionsForLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteManagedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "TerminateManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:ManagedResourceOperator" : "ecs.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonECSInfrastructureRoleforExpressGatewayServices

Deskripsi: Izin ini memungkinkan Amazon ECS untuk secara otomatis menyediakan dan mengelola komponen infrastruktur yang diperlukan untuk Layanan Express Gateway, termasuk penyeimbangan beban, grup keamanan, sertifikat SSL, dan konfigurasi penskalaan otomatis.

`AmazonECSInfrastructureRoleforExpressGatewayServices`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonECSInfrastructureRoleforExpressGatewayServices` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 12 November 2025, 20:34 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRoleforExpressGatewayServices`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ServiceLinkedRoleCreateOperations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ecs.application-autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ELBOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateRule",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:ModifyRule",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteRule",
        "elasticloadbalancing:DeleteListener"
      ],
      "Resource" : [
```

```
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateELBResources",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:AddTags",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateLoadBalancer",
            "CreateListener",
            "CreateRule",
            "CreateTargetGroup"
          ]
        }
      }
    },
    {
      "Sid" : "BlanketAllowCreateSecurityGroupsInVPCs",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "CreateSecurityGroupResourcesWithTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupEgress",
```

```
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ModifySecurityGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateEC2Resources",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
```

```
            "CreateSecurityGroup",
            "AuthorizeSecurityGroupIngress",
            "AuthorizeSecurityGroupEgress"
          ]
        }
      }
    },
    {
      "Sid" : "CertificateOperations",
      "Effect" : "Allow",
      "Action" : [
        "acm:RequestCertificate",
        "acm:AddTagsToCertificate",
        "acm:DeleteCertificate",
        "acm:DescribeCertificate"
      ],
      "Resource" : [
        "arn:aws:acm:*:*:certificate/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingCreateOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:TagResource",
        "application-autoscaling:DeregisterScalableTarget"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingPolicyOperations",
```

```
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DeleteScalingPolicy"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "ecs"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScalingActivities"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*"
      ]
    },
    {
      "Sid" : "CloudWatchAlarmCreateOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CloudWatchAlarmOperations",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ELBReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VPCReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsCreateOperations",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
```

```
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonECSInfrastructureRoleForGatewayHostSharedALB

Deskripsi: Kebijakan default untuk Peran Infrastruktur Amazon ECS untuk Layanan Gateway Layanan Amazon ECS.

`AmazonECSInfrastructureRoleForGatewayHostSharedALB`Badalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonECSInfrastructureRoleForGatewayHostSharedALB` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 September 2026, 21:17 UTC
- Waktu teredit: 25 September 2026, 21:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRoleForGatewayHostSharedALB`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ServiceLinkedRoleCreateOperations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticloadbalancing.amazonaws.com/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ELBOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateRule",
```

```
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:ModifyRule",
        "elasticloadbalancing:SetRulePriorities",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteRule",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:SetSecurityGroups"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateELBResources",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:AddTags",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateLoadBalancer",
            "CreateListener",
            "CreateRule",
            "CreateTargetGroup"
```

```
        ]
      }
    }
  },
  {
    "Sid" : "BlanketAllowCreateSecurityGroupsInVPCs",
    "Effect" : "Allow",
    "Action" : "ec2:CreateSecurityGroup",
    "Resource" : "arn:aws:ec2:*:*:vpc/*"
  },
  {
    "Sid" : "CreateSecurityGroupResourcesWithTags",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:security-group-rule/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/AmazonECSManaged" : "true"
      }
    }
  },
  {
    "Sid" : "ModifySecurityGroupOperations",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:DeleteSecurityGroup",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:vpc/*"
    ],
    "Condition" : {
      "StringEquals" : {
```

```
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateEC2Resources",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "AuthorizeSecurityGroupIngress",
            "AuthorizeSecurityGroupEgress"
          ]
        }
      }
    },
    {
      "Sid" : "CertificateOperations",
      "Effect" : "Allow",
      "Action" : [
        "acm:AddTagsToCertificate",
        "acm:DeleteCertificate"
      ],
      "Resource" : "arn:aws:acm:*:*:certificate/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CertificateCreateOperations",
      "Effect" : "Allow",
      "Action" : [
        "acm:RequestCertificate"
      ],
      "Resource" : "arn:aws:acm:*:*:certificate/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CertificateReadOperations",
      "Effect" : "Allow",
      "Action" : "acm:DescribeCertificate",
      "Resource" : "arn:aws:acm:*:*:certificate/*"
    },
    {
      "Sid" : "WAFAssociationOnALBs",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:AssociateWebACL",
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : "arn:aws:wafv2:*:*:regional/webacl/*/*"
    },
    {
      "Sid" : "ELBSetWebACLOnALBs",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateWebACLAssociation",
        "elasticloadbalancing:DeleteWebACLAssociation",
        "elasticloadbalancing:SetWebACL"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "WAFReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:wafv2:*:*:regional/webacl/*/*"
    },
    {
      "Sid" : "ELBGetWebACLOnALBs",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:GetLoadBalancerWebACL",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
```

```
    },
    {
      "Sid" : "ELBReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VPCReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonECSInfrastructureRolePolicyForLoadBalancers

Deskripsi: Menyediakan akses ke sumber daya AWS layanan lain yang diperlukan untuk mengelola penyeimbang beban yang terkait dengan beban kerja ECS atas nama Anda.

`AmazonECSInfrastructureRolePolicyForLoadBalancers`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonECSInfrastructureRolePolicyForLoadBalancers` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Juli 2025, 16:37 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForLoadBalancers`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ELBReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "TargetGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
    },
    {
      "Sid" : "ALBModifyListeners",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:ModifyListener",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*"
      ]
    },
    {
      "Sid" : "NLBModifyListeners",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:ModifyListener",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/net/*/*/*"
      ]
    },
    {
      "Sid" : "ALBModifyRules",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:ModifyRule",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonECSInfrastructureRolePolicyForManagedInstances

Deskripsi: Menyediakan akses ECS untuk membuat dan mengelola sumber daya terkelola EC2

`AmazonECSInfrastructureRolePolicyForManagedInstances`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonECSInfrastructureRolePolicyForManagedInstances` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 September 2025, 18:04 UTC
- Waktu teredit: 15 September 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForManagedInstances`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateLaunchTemplateForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CreateLaunchTemplateVersionsForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ProvisionEC2InstancesForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "CreateFleetForSupportingResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Sid" : "CreateFleetForECSManagedLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "RunInstancesForECSManagedLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesForSupportingResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:resource-groups:*:*:group/*"
      ]
    },
    {
      "Sid" : "TagOnCreateEC2ResourcesForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateFleet",
```

```
            "CreateLaunchTemplate",
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "PassInstanceRoleForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/ecsInstanceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.*"
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRoleForEC2Spot",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/
AWSServiceRoleForEC2Spot"
      ]
    },
    {
      "Sid" : "DescribeEC2ResourcesManagedByECS",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeCapacityReservations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListResourceGroupResources",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerS

Deskripsi: Menyediakan akses administratif ke Otoritas Sertifikat AWS Pribadi, Manajer Rahasia, dan lainnya yang Layanan AWS diperlukan untuk mengelola fitur ECS Service Connect TLS atas nama Anda.

`AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Januari 2024, 20:08 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "TagOnCreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RotateTLSCertificateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:UpdateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecretVersionStage"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "ecs-sc",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DescribeTLSCertificateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManagePrivateCertificateAuthority",
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:GetCertificate",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ManagePrivateCertificateAuthorityForIssuingEndEntityCertificate",
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true",
          "acm-pca:TemplateArn" : "arn:aws:acm-pca:::template/EndEntityCertificate/V1"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonECSInfrastructureRolePolicyForVolumes

Deskripsi: Menyediakan akses ke sumber daya AWS layanan lain yang diperlukan untuk mengelola volume yang terkait dengan beban kerja ECS atas nama Anda.

`AmazonECSInfrastructureRolePolicyForVolumes`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonECSInfrastructureRolePolicyForVolumes` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 10 Januari 2024, 22:56 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
```

```
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEBSManagedVolumeFromSnapshot",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*"
    },
    {
      "Sid" : "TagOnCreateVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVolume",
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeVolumesForLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstancesForAttachingVolume",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageEBSVolumeLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ManageVolumeAttachmentsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DeleteEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:ResourceTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonECSInfrastructureRolePolicyForVpcLattice

Deskripsi: Menyediakan akses ke sumber daya AWS layanan lain yang diperlukan untuk mengelola fitur VPC Lattice dalam beban kerja ECS atas nama Anda.

`AmazonECSInfrastructureRolePolicyForVpcLattice`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonECSInfrastructureRolePolicyForVpcLattice` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 November 2024, 20:02 UTC
- Waktu teredit: 29 September 2026, 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForVpcLattice`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManagedVpcLatticeTargetRegistration",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:RegisterTargets",
        "vpc-lattice:DeregisterTargets"
      ],
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:targetgroup/*"
      ]
    },
    {
      "Sid" : "DescribeVpcLatticeTargetGroup",
      "Effect" : "Allow",
      "Action" : "vpc-lattice:GetTargetGroup",
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:targetgroup/*"
      ]
    },
    {
      "Sid" : "ListVpcLatticeTargets",
      "Effect" : "Allow",
      "Action" : "vpc-lattice:ListTargets",
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:targetgroup/*"
      ]
    },
    {
      "Sid" : "GetRule",
      "Effect" : "Allow",
      "Action" : "vpc-lattice:GetRule",
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:service/*/listener/*/rule/*"
      ]
    },
    {
      "Sid" : "UpdateRule",
      "Effect" : "Allow",
```

```
      "Action" : "vpc-lattice:UpdateRule",
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:service/*/listener/*/rule/*"
      ]
    },
    {
      "Sid" : "UpdateListener",
      "Effect" : "Allow",
      "Action" : "vpc-lattice:UpdateListener",
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:service/*/listener/*"
      ]
    },
    {
      "Sid" : "DescribeEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonECSInstanceRolePolicyForManagedInstances

Deskripsi: Kebijakan default untuk Peran Instans Amazon ECS untuk Instans Terkelola Amazon ECS.

`AmazonECSInstanceRolePolicyForManagedInstances`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonECSInstanceRolePolicyForManagedInstances` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 September 2025, 23:49 UTC
- Waktu teredit: 02 Juli 2026, 02:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInstanceRolePolicyForManagedInstances`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSAgentDiscoverPollEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DiscoverPollEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECSAgentRegisterPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ecs:RegisterContainerInstance"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/*"
    },
    {
      "Sid" : "ECSAgentPollPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:Poll"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:container-instance/*",
        "arn:aws:ecs:*:*:task-set/*"
      ]
    },
    {
      "Sid" : "ECSAgentTelemetryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:StartTelemetrySession",
        "ecs:PutSystemLogEvents"
      ],
      "Resource" : "arn:aws:ecs:*:*:container-instance/*"
    },
    {
      "Sid" : "ECSAgentStateChangePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:SubmitAttachmentStateChanges",
        "ecs:SubmitTaskStateChange"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonECSServiceRolePolicy

Deskripsi: Kebijakan untuk mengaktifkan Amazon ECS untuk mengelola cluster Anda.

`AmazonECSServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 14 Oktober 2017, 01:18 UTC
- Waktu teredit: 22 April 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v24 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSTaskManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:AssociateTrunkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
```

```
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:Describe*",
        "ec2:DetachNetworkInterface",
        "ec2:DisassociateTrunkInterface",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:Get*",
        "route53:List*",
        "route53:UpdateHealthCheck",
        "servicediscovery:DeregisterInstance",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:UpdateInstanceCustomHealthStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingManagement",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DeletePolicy",
        "autoscaling:PutScalingPolicy",
        "autoscaling:SetInstanceProtection",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:PutLifecycleHook",
        "autoscaling:DeleteLifecycleHook",
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:RecordLifecycleActionHeartbeat",
        "autoscaling:TerminateInstanceInAutoScalingGroup"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "autoscaling:ResourceTag/AmazonECSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "AutoScalingPlanManagement",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling-plans:CreateScalingPlan",
        "autoscaling-plans:DeleteScalingPlan",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:DescribeScalingPlanResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/ecs-managed-*"
    },
    {
      "Sid" : "EventBridgeRuleManagement",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CWAlarmManagement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ECSTagging",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "CWLogGroupManagement",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/*"
    },
    {
      "Sid" : "CWLogStreamManagement",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/*:log-stream:*"
    },
    {
      "Sid" : "ExecuteCommandSessionManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeSessions"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ExecuteCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task/*",
        "arn:aws:ssm:*:*:document/AmazonECS-ExecuteInteractiveCommand"
      ]
    },
    {
      "Sid" : "OpenDataChannel",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "CloudMapResourceCreation",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:CreateHttpNamespace",
        "servicediscovery:CreateService"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonECSManaged"
          ]
        }
      }
    },
    {
      "Sid" : "CloudMapResourceTagging",
```

```
      "Effect" : "Allow",
      "Action" : "servicediscovery:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AmazonECSManaged" : "*"
        }
      }
    },
    {
      "Sid" : "CloudMapResourceDeletion",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DeleteService"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonECSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "CloudMapResourceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudMapResourceAttributeManagement",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:UpdateServiceAttributes"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonECSManaged" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "ReadOnlyPermissionsForInstanceEventWindows",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceEventWindows"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonECSTaskExecutionRolePolicy

Deskripsi: Menyediakan akses ke sumber daya AWS layanan lain yang diperlukan untuk menjalankan tugas Amazon ECS

`AmazonECSTaskExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonECSTaskExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 16 November 2017, 18:48 UTC
- Waktu teredit: 16 November 2017, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEFSCSIDriverPolicy

Deskripsi: Menyediakan akses manajemen ke sumber daya EFS dan akses baca ke EC2

`AmazonEFSCSIDriverPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEFSCSIDriverPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 25 Juli 2023, 20:10 UTC
- Waktu teredit: 25 Juli 2023, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateAccessPoint",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:CreateAccessPoint"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "efs.csi.aws.com/cluster"
        }
      }
    },
    {
      "Sid" : "AllowTagNewAccessPoints",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticfilesystem:CreateAction" : "CreateAccessPoint"
        },
        "Null" : {
          "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "efs.csi.aws.com/cluster"
        }
      }
    },
    {
      "Sid" : "AllowDeleteAccessPoint",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:DeleteAccessPoint",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/efs.csi.aws.com/cluster" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEKS_CNI_Policy

Deskripsi: Kebijakan ini menyediakan Plugin Amazon VPC CNI (amazon-vpc-cni-k8s) izin yang diperlukan untuk mengubah konfigurasi alamat IP pada node pekerja EKS Anda. Kumpulan izin ini memungkinkan CNI untuk membuat daftar, menjelaskan, dan memodifikasi Antarmuka Jaringan Elastis atas nama Anda. Informasi lebih lanjut tentang Plugin AWS VPC CNI tersedia di sini: https://github.com/aws/amazon-vpc-cni-k8s

`AmazonEKS_CNI_Policy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKS_CNI_Policy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2018, 21:07 UTC
- Waktu teredit: 04 Maret 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEKSCNIPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEKSCNIPolicyENITag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEKSBlockStoragePolicy

Deskripsi: Kebijakan yang dilampirkan ke Peran Cluster EKS yang memberikan izin untuk mengelola sumber daya penyimpanan blok cluster.

`AmazonEKSBlockStoragePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSBlockStoragePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Oktober 2024, 20:18 UTC
- Waktu teredit: 30 Oktober 2024, 20:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSBlockStoragePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume",
```

```
        "ec2:ModifyVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "CSIVolumeName",
            "ebs.csi.eks.amazonaws.com/cluster",
            "kubernetes.io/cluster/*",
            "kubernetes.io/created-for/*",
            "Name",
            "KubernetesCluster"
```

```
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "CSIVolumeSnapshotName",
            "ebs.csi.eks.amazonaws.com/cluster",
            "kubernetes.io/cluster/*",
            "Name"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEKSBlockStoragePolicyV2

Deskripsi: Kebijakan yang dilampirkan ke Peran Cluster EKS yang memberikan izin untuk mengelola sumber daya penyimpanan blok cluster.

`AmazonEKSBlockStoragePolicyV2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSBlockStoragePolicyV2` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Mei 2026, 16:27 UTC
- Waktu teredit: 11 Mei 2026, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSBlockStoragePolicyV2`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:ModifyVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
```

```
            "eks:eks-cluster-name",
            "CSIVolumeName",
            "ebs.csi.eks.amazonaws.com/cluster",
            "kubernetes.io/cluster/*",
            "kubernetes.io/created-for/*",
            "Name",
            "KubernetesCluster"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "CSIVolumeSnapshotName",
            "ebs.csi.eks.amazonaws.com/cluster",
            "kubernetes.io/cluster/*",
            "Name"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEKSClusterPolicy

Deskripsi: Kebijakan ini memberikan Kubernetes izin yang diperlukan untuk mengelola sumber daya atas nama Anda. Kubernetes memerlukan Ec2:CreateTags izin untuk menempatkan informasi identifikasi pada sumber daya EC2 termasuk namun tidak terbatas pada Instans, Grup Keamanan, dan Antarmuka Jaringan Elastis.

`AmazonEKSClusterPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSClusterPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2018, 21:06 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSClusterPolicy`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEKSClusterPolicy",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:UpdateAutoScalingGroup",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateRoute",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteRoute",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
```

```
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DetachVolume",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyVolume",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeInstanceTopology",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:AttachLoadBalancerToSubnets",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateLoadBalancerPolicy",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancerListeners",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DetachLoadBalancerFromSubnets",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:ModifyTargetGroupAttributes",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
```

```
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEKSClusterPolicySLRCreate",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonEKSClusterPolicyENIDelete",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/eks:eni:owner" : "amazon-vpc-cni"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEKSComputePolicy

Deskripsi: Kebijakan yang dilampirkan ke Peran Cluster EKS yang memberikan izin untuk mengelola sumber daya komputasi cluster.

`AmazonEKSComputePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSComputePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 November 2024, 21:46 UTC
- Waktu yang diedit: 18 Mei 2026, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSComputePolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances",
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "StringLike" : {
          "aws:RequestTag/eks:kubernetes-node-class-name" : "*",
          "aws:RequestTag/eks:kubernetes-node-pool-name" : "*"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "eks:kubernetes-node-class-name",
            "eks:kubernetes-node-pool-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateFleet",
            "RunInstances",
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:AddRoleToInstanceProfile",
      "Resource" : "arn:aws:iam::*:instance-profile/eks*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/
AWSServiceRoleForEC2Spot"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "ec2:DescribeCapacityReservations",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEKSConnectorServiceRolePolicy

Deskripsi: Kebijakan ini memungkinkan Amazon EKS mengelola AWS sumber daya untuk konektor EKS

`AmazonEKSConnectorServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 04 September 2021, 20:31 UTC
- Waktu teredit: 15 Oktober 2025, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSConnectorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessSSMService",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateActivation",
        "ssm:DescribeInstanceInformation",
        "ssm:DeleteActivation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConnectorAgentStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*",
        "arn:aws:ssm:*::document/AmazonEKS-ExecuteNonInteractiveCommand"
      ]
    },
    {
      "Sid" : "ConnectorAgentDeregister",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeregisterManagedInstance"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*"
      ]
```

```
    },
    {
      "Sid" : "PassAnyRoleToSsm",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PutManagedEventRule",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "eks-connector.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "events:source" : "aws.ssm"
        }
      }
    },
    {
      "Sid" : "PutManagedEventTarget",
      "Effect" : "Allow",
      "Action" : "events:PutTargets",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "eks-connector.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OpenDataChannel",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEKSDashboardConsoleReadOnly

Deskripsi: Menyediakan akses baca saja untuk melihat dasbor di konsol Amazon EKS. Dasbor mengumpulkan informasi tentang beberapa cluster dan sumber daya terkait menggunakan AWS Organisasi.

`AmazonEKSDashboardConsoleReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSDashboardConsoleReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Juni 2025, 17:22 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSDashboardConsoleReadOnly`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEKSDashboardReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListDashboardData",
        "eks:ListDashboardResources",
        "eks:DescribeClusterVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonOrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonOrganizationsDelegatedAdmin",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "eks.amazonaws.com"
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEKSDashboardServiceRolePolicy

Deskripsi: Kebijakan ini memungkinkan Dasbor Amazon EKS untuk mengakses dan menampilkan informasi di seluruh organisasi. Kebijakan ini memungkinkan layanan Dasbor EKS untuk mengumpulkan informasi tentang struktur dan akun Organisasi Anda AWS .

`AmazonEKSDashboardServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 08 Mei 2025, 19:07 UTC
- Waktu teredit: 08 Mei 2025, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSDashboardServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOrganizationsReadActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEKSFargatePodExecutionRolePolicy

Deskripsi: Menyediakan akses ke sumber daya AWS layanan lain yang diperlukan untuk menjalankan pod Amazon EKS di AWS Fargate

`AmazonEKSFargatePodExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSFargatePodExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 November 2019, 04:34 UTC
- Waktu teredit: 22 November 2019, 04:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEKSForFargateServiceRolePolicy

Deskripsi: Kebijakan ini memberikan izin yang diperlukan kepada Amazon EKS untuk menjalankan tugas fargate

`AmazonEKSForFargateServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 22 November 2019, 04:36 UTC
- Waktu teredit: 22 November 2019, 04:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSForFargateServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEKSLoadBalancingPolicy

Deskripsi: Kebijakan yang dilampirkan ke Peran Cluster EKS yang memberikan izin untuk mengelola sumber daya penyeimbang beban cluster.

`AmazonEKSLoadBalancingPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSLoadBalancingPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Oktober 2024, 20:18 UTC
- Waktu teredit: 20 Agustus 2026, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSLoadBalancingPolicy`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateRule",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "ingress.eks.amazonaws.com/stack",
            "ingress.eks.amazonaws.com/resource",
```

```
            "service.eks.amazonaws.com/stack",
            "service.eks.amazonaws.com/resource",
            "gateway.eks.amazonaws.com.alb/stack",
            "gateway.eks.amazonaws.com.alb/resource",
            "gateway.eks.amazonaws.com.nlb/stack",
            "gateway.eks.amazonaws.com.nlb/resource"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group-rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
```

```
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/Name" : "eks-cluster-sg*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateLoadBalancer",
            "CreateTargetGroup",
            "CreateListener",
            "CreateRule"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "AuthorizeSecurityGroupIngress"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:SetIpAddressType",
        "elasticloadbalancing:SetSecurityGroups",
        "elasticloadbalancing:SetSubnets",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:ModifyTargetGroupAttributes",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:ModifyListenerAttributes",
        "elasticloadbalancing:RemoveListenerCertificates",
        "elasticloadbalancing:ModifyRule",
        "elasticloadbalancing:ModifyIpPools",
        "elasticloadbalancing:ModifyCapacityReservation",
        "elasticloadbalancing:DescribeLoadBalancers"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "wafv2:AssociateWebACL",
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "shield:CreateProtection",
        "shield:DeleteProtection"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "shield:TagResource"
      ],
      "Resource" : "arn:aws:shield::*:protection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "ingress.eks.amazonaws.com/stack",
            "ingress.eks.amazonaws.com/resource",
            "service.eks.amazonaws.com/stack",
            "service.eks.amazonaws.com/resource",
            "gateway.eks.amazonaws.com.alb/stack",
            "gateway.eks.amazonaws.com.alb/resource",
            "gateway.eks.amazonaws.com.nlb/stack",
            "gateway.eks.amazonaws.com.nlb/resource"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPoolClient",
        "acm:ListCertificates",
        "acm:DescribeCertificate",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListWebACLs",
```

```
        "elasticloadbalancing:SetWebAcl",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:SetRulePriorities"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeIpamPools"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEKSLocalOutpostClusterPolicy

Deskripsi: Kebijakan ini memberikan izin ke instans bidang kontrol cluster lokal EKS yang berjalan di akun Anda untuk mengelola sumber daya atas nama Anda.

`AmazonEKSLocalOutpostClusterPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSLocalOutpostClusterPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Agustus 2022, 21:56 UTC
- Waktu teredit: 24 Oktober 2024, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeAvailabilityZones",
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:DescribeInstanceProperties",
        "ssm:DescribeDocumentParameters",
        "ssm:ListInstanceAssociations",
        "ssm:RegisterManagedInstance",
        "ssm:UpdateInstanceInformation",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:PutComplianceItems",
        "ssm:PutInventory",
        "ecr-public:GetAuthorizationToken",
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/eks/*",
        "arn:aws:ecr:*:*:repository/bottlerocket-admin",
        "arn:aws:ecr:*:*:repository/bottlerocket-control-eks",
```

```
        "arn:aws:ecr:*:*:repository/diagnostics-collector-eks",
        "arn:aws:ecr:*:*:repository/kubelet-config-updater"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:*:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEKSLocalOutpostServiceRolePolicy

Deskripsi: Mengizinkan Amazon EKS Local untuk menelepon AWS layanan atas nama Anda.

`AmazonEKSLocalOutpostServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 23 Agustus 2022, 21:53 UTC
- Waktu teredit: 26 Juni 2025, 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSLocalOutpostServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeVpcAttribute",
        "ec2:DescribePlacementGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:TerminateInstances",
        "ec2:GetConsoleOutput"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*",
            "eks*"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface",
            "CreateSecurityGroup",
            "RunInstances"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
```

```
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*",
            "eks*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:DeleteSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:DescribeSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks-local-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ssm:*::document/AmazonEKS-ControlPlaneInstanceProxy"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ResumeSession",
        "ssm:TerminateSession"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:GetOutpost"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEKSMCPReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke layanan Amazon EKS MCP. Kebijakan ini memberikan izin untuk hanya menggunakan alat baca-saja di layanan EKS MCP yang dimaksudkan untuk pengamatan, pemecahan masalah, mengambil informasi sumber daya EKS, dan mendapatkan saran. EKS-optimized

`AmazonEKSMCPReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSMCPReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 November 2025, 17:19 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSMCPReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:ListClusters",
        "eks:DescribeNodegroup",
        "eks:ListNodegroups",
        "eks:DescribeAddon",
        "eks:ListAddons",
        "eks:DescribeAccessEntry",
        "eks:ListAccessEntries",
        "eks:DescribeInsight",
        "eks:ListInsights",
        "eks:AccessKubernetesApi"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks-mcp:InvokeMcp",
        "eks-mcp:CallReadOnlyTool"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEKSNetworkingPolicy

Deskripsi: Kebijakan yang dilampirkan ke Peran Cluster EKS yang memberikan izin untuk mengelola sumber daya jaringan cluster.

`AmazonEKSNetworkingPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSNetworkingPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Oktober 2024, 22:34 UTC
- Waktu teredit: 21 Agustus 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSNetworkingPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "StringLike" : {
          "aws:RequestTag/eks:kubernetes-cni-node-name" : "*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "eks:kubernetes-cni-node-name",
            "sgp.eks.amazonaws.com/instance-id",
            "sgp.eks.amazonaws.com/trunk-eni-id",
            "sgp.eks.amazonaws.com/vlan-id",
            "sgp.eks.amazonaws.com/managed",
            "sgp.eks.amazonaws.com/policy-ref"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:ModifyNetworkInterfaceAttribute",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateTrunkInterface",
        "ec2:DisassociateTrunkInterface"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEKSServicePolicy

Deskripsi: Kebijakan ini memungkinkan Amazon Elastic Container Service for Kubernetes membuat dan mengelola sumber daya yang diperlukan untuk mengoperasikan Cluster EKS.

`AmazonEKSServicePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSServicePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2018, 21:08 UTC
- Waktu teredit: 14 Oktober 2024, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSServicePolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "iam:ListAttachedRolePolicies",
        "eks:UpdateClusterVersion",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : "eks-cluster-*"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "route53:AssociateVPCWithHostedZone",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/eks.amazonaws.com/
AWSServiceRoleForAmazonEKS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "eks.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEKSServiceRolePolicy

Deskripsi: Service-Linked Peran yang diperlukan untuk Amazon EKS untuk memang AWS gil layanan atas nama Anda.

`AmazonEKSServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 21 Februari 2020, 20:10 UTC
- Waktu teredit: 01 Oktober 2026, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v28 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkAcls",
        "ec2:GetCoipPoolUsage",
        "ec2:GetSecurityGroupsForVpc",
        "eks:DescribeCluster",
        "ec2:DescribeIpamPools",
        "ec2:DescribeTrunkInterfaceAssociations",
        "elasticloadbalancing:DescribeListenerAttributes",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
```

```
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeSSLPolicies",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DescribeTrustStores",
        "elasticloadbalancing:DescribeCapacityReservation",
        "iam:ListAttachedRolePolicies",
        "pricing:GetProducts",
        "shield:GetSubscriptionState",
        "shield:DescribeProtection",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/Name" : "eks-cluster-sg*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
```

```
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : "eks-cluster-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "route53:AssociateVPCWithHostedZone",
      "Resource" : "arn:aws:route53:::hostedzone/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : "AWS/EKS"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateCertificateAuthority",
        "eks:DeleteCertificateAuthority",
        "eks:ActivateCertificateAuthority"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateAccessEntry",
        "eks:DeleteAccessEntry"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "eks:accessEntryType" : "STANDARD"
        },
        "ArnLike" : {
          "eks:principalArn" : "arn:aws:iam::*:role/aws-service-role/eks.amazonaws.com/
AWSServiceRoleForAmazonEKS"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:ListAssociatedAccessPolicies"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*/role/${aws:PrincipalAccount}/
AWSServiceRoleForAmazonEKS/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DisassociateAccessPolicy"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*/role/${aws:PrincipalAccount}/
AWSServiceRoleForAmazonEKS/*",
      "Condition" : {
        "StringEquals" : {
          "eks:policyArn" : [
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSComputePolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSComputeClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSNetworkingPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSNetworkingClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSLoadBalancingPolicy",
            "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSLoadBalancingClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSBlockStoragePolicy",
            "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSBlockStorageClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSHybridPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSEventPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSPodIdentityPolicy"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "eks:DescribeAccessEntry",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "eks:accessEntryType" : "EC2"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/EKS*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.ec2",
            "aws.health"
          ]
        },
        "StringEquals" : {
          "events:ManagedBy" : [
            "eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "events:PutTargets",
      "Resource" : "arn:aws:events:*:*:rule/EKS*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
```

```
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:ListInstanceProfiles"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "arn:aws:iam::*:instance-profile/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:TerminateInstances",
        "ec2:RebootInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:TerminateInstances",
        "ec2:RebootInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : [
            "eks.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteRule",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteTargetGroup",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEKSVPCResourceController

Deskripsi: Kebijakan yang digunakan oleh VPC Resource Controller untuk mengelola ENI dan IP untuk node pekerja.

`AmazonEKSVPCResourceController`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSVPCResourceController` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Agustus 2020, 00:55 UTC
- Waktu teredit: 12 Agustus 2020, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSVPCResourceController`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterfacePermission",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "ec2:ResourceTag/eks:eni:owner" : "eks-vpc-resource-controller"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:AttachNetworkInterface",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEKSWorkerNodeMinimalPolicy

Deskripsi: Kebijakan ini memungkinkan node pekerja Amazon EKS untuk terhubung ke Cluster Amazon EKS.

`AmazonEKSWorkerNodeMinimalPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSWorkerNodeMinimalPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Oktober 2024, 20:03 UTC
- Waktu teredit: 02 Oktober 2024, 20:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSWorkerNodeMinimalPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkerNodePermissions",
      "Effect" : "Allow",
      "Action" : [
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEKSWorkerNodePolicy

Deskripsi: Kebijakan ini memungkinkan node pekerja Amazon EKS untuk terhubung ke Cluster Amazon EKS.

`AmazonEKSWorkerNodePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSWorkerNodePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2018, 21:09 UTC
- Waktu teredit: 27 November 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkerNodePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcs",
        "eks:DescribeCluster",
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElastiCacheFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon ElastiCache melalui Konsol Manajemen AWS.

`AmazonElastiCacheFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElastiCacheFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 28 November 2023, 03:49 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheManagementActions",
      "Effect" : "Allow",
      "Action" : "elasticache:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/elasticache.amazonaws.com/
AWSServiceRoleForElastiCache",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticache.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateVPCEndpoints",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
        }
```

```
      }
    },
    {
      "Sid" : "AllowAccessToElastiCacheTaggedVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
    },
    {
      "Sid" : "TagVPCEndpointsOnCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/AmazonElastiCacheManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAccessToEc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowAccessToCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToAutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScalingActivities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListLogDeliveryStreams",
      "Effect" : "Allow",
      "Action" : [
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowAccessToOutposts",
      "Effect" : "Allow",
      "Action" : [
        "outposts:ListOutposts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToSNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElastiCacheReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon ElastiCache melalui Konsol Manajemen AWS.

`AmazonElastiCacheReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElastiCacheReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticache:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElasticContainerRegistryPublicFullAccess

Deskripsi: Menyediakan akses administratif ke Amazon ECR Sumber daya publik

`AmazonElasticContainerRegistryPublicFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticContainerRegistryPublicFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2020, 17:25 UTC
- Waktu teredit: 01 Desember 2020, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:*",
        "sts:GetServiceBearerToken"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElasticContainerRegistryPublicPowerUser

Deskripsi: Menyediakan akses penuh ke repositori Amazon ECR Public, tetapi tidak mengizinkan penghapusan repositori atau perubahan kebijakan.

`AmazonElasticContainerRegistryPublicPowerUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticContainerRegistryPublicPowerUser` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2020, 16:16 UTC
- Waktu teredit: 01 Desember 2020, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicPowerUser`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken",
        "sts:GetServiceBearerToken",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:DescribeRepositories",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:InitiateLayerUpload",
        "ecr-public:UploadLayerPart",
        "ecr-public:CompleteLayerUpload",
        "ecr-public:PutImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElasticContainerRegistryPublicReadOnly

Deskripsi: Menyediakan akses baca-saja ke repositori Amazon ECR Public.

`AmazonElasticContainerRegistryPublicReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticContainerRegistryPublicReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2020, 17:27 UTC
- Waktu teredit: 01 Desember 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken",
        "sts:GetServiceBearerToken",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:DescribeRepositories",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRegistryCatalogData"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElasticFileSystemClientFullAccess

Deskripsi: Menyediakan akses klien root ke sistem file Amazon EFS

`AmazonElasticFileSystemClientFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticFileSystemClientFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 Januari 2020, 16:27 UTC
- Waktu teredit: 13 Januari 2020, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElasticFileSystemClientReadOnlyAccess

Deskripsi: Menyediakan akses klien baca saja ke sistem file Amazon EFS

`AmazonElasticFileSystemClientReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticFileSystemClientReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 13 Januari 2020, 16:24 UTC
- Waktu teredit: 13 Januari 2020, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElasticFileSystemClientReadWriteAccess

Deskripsi: Menyediakan akses klien baca dan tulis ke sistem file Amazon EFS

`AmazonElasticFileSystemClientReadWriteAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticFileSystemClientReadWriteAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 Januari 2020, 16:21 UTC
- Waktu teredit: 13 Januari 2020, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElasticFileSystemFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon EFS melalui Konsol Manajemen AWS.

`AmazonElasticFileSystemFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticFileSystemFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2015, 16:22 UTC
- Waktu teredit: 07 November 2024, 19:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "ElasticFileSystemFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricData",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:CreateTags",
        "elasticfilesystem:CreateAccessPoint",
        "elasticfilesystem:CreateReplicationConfiguration",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget",
        "elasticfilesystem:DeleteTags",
        "elasticfilesystem:DeleteAccessPoint",
        "elasticfilesystem:DeleteFileSystemPolicy",
        "elasticfilesystem:DeleteReplicationConfiguration",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:ModifyMountTargetSecurityGroups",
        "elasticfilesystem:PutAccountPreferences",
        "elasticfilesystem:PutBackupPolicy",
        "elasticfilesystem:PutLifecycleConfiguration",
        "elasticfilesystem:PutFileSystemPolicy",
        "elasticfilesystem:UpdateFileSystem",
```

```
        "elasticfilesystem:UpdateFileSystemProtection",
        "elasticfilesystem:TagResource",
        "elasticfilesystem:UntagResource",
        "elasticfilesystem:ListTagsForResource",
        "elasticfilesystem:Backup",
        "elasticfilesystem:Restore",
        "elasticfilesystem:ReplicationRead",
        "elasticfilesystem:ReplicationWrite",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleForEFS",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "elasticfilesystem.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForEFS",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "elasticfilesystem.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElasticFileSystemReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon EFS melalui Konsol Manajemen AWS.

`AmazonElasticFileSystemReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticFileSystemReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2015, 16:25 UTC
- Waktu teredit: 07 November 2024, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticFileSystemReadOnlyAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricData",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:ListTagsForResource",
        "elasticfilesystem:ReplicationRead",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElasticFileSystemServiceRolePolicy

Deskripsi: Mengizinkan Amazon Elastic File System mengelola AWS sumber daya atas nama Anda

`AmazonElasticFileSystemServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 05 November 2019, 16:52 UTC
- Waktu teredit: 07 November 2024, 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-storage:MountCapsule",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:ModifyNetworkInterfaceAttribute",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupVault",
        "backup:PutBackupVaultAccessPolicy"
      ],
      "Resource" : [
        "arn:aws:backup:*:*:backup-vault:aws/efs/automatic-backup-vault"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupPlan",
        "backup:CreateBackupSelection"
      ],
      "Resource" : [
        "arn:aws:backup:*:*:backup-plan:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/backup.amazonaws.com/
AWSServiceRoleForBackup"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:CreateReplicationConfiguration",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:DeleteReplicationConfiguration",
        "elasticfilesystem:ReplicationRead",
        "elasticfilesystem:ReplicationWrite"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElasticFileSystemsUtils

Deskripsi: Memungkinkan pelanggan menggunakan Manajer AWS Sistem untuk secara otomatis mengelola paket utilitas Amazon EFS (amazon-efs-utils) pada instans EC2 mereka, dan menggunakannya CloudWatchLog untuk mendapatkan notifikasi pemasangan sistem file EFS. success/failure

`AmazonElasticFileSystemsUtils`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticFileSystemsUtils` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 September 2020, 15:16 UTC
- Waktu teredit: 07 April 2026, 13:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
```

```
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "efs-utils/S3Files",
            "efs-utils/EFS"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElasticMapReduceEditorsRole

Deskripsi: Kebijakan default untuk peran layanan Amazon Elastic MapReduce Editors.

`AmazonElasticMapReduceEditorsRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticMapReduceEditorsRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 16 November 2018, 21:55 UTC
- Waktu teredit: 09 Februari 2023, 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceEditorsRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListSteps"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:elasticmapreduce:editor-id",
            "aws:elasticmapreduce:job-flow-id"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElasticMapReduceforAutoScalingRole

Deskripsi: Amazon Elastic MapReduce untuk Penskalaan Otomatis. Peran untuk mengizinkan Auto Scaling menambah dan menghapus instance dari cluster EMR Anda.

`AmazonElasticMapReduceforAutoScalingRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticMapReduceforAutoScalingRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 18 November 2016, 01:09 UTC
- Waktu teredit: 18 November 2016, 01:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElasticMapReduceforEC2Role

Deskripsi: Kebijakan default untuk peran layanan Amazon Elastic MapReduce untuk EC2.

`AmazonElasticMapReduceforEC2Role`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticMapReduceforEC2Role` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 11 Agustus 2017, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "cloudwatch:*",
        "dynamodb:*",
        "ec2:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSteps",
        "kinesis:CreateStream",
        "kinesis:DeleteStream",
        "kinesis:DescribeStream",
        "kinesis:GetRecords",
        "kinesis:GetShardIterator",
        "kinesis:MergeShards",
        "kinesis:PutRecord",
        "kinesis:SplitShard",
        "rds:Describe*",
        "s3:*",
        "sdb:*",
        "sns:*",
        "sqs:*",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue:DeleteTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersions",
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:UpdatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
```

```
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue:CreateUserDefinedFunction",
        "glue:UpdateUserDefinedFunction",
        "glue:DeleteUserDefinedFunction",
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElasticMapReduceFullAccess

Deskripsi: Kebijakan ini berada di jalur penghentian. Lihat dokumentasi untuk panduan: https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html. Menyediakan akses penuh ke Amazon Elastic MapReduce dan layanan dasar yang diperlukan seperti EC2 dan S3

`AmazonElasticMapReduceFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticMapReduceFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 11 September 2026, 17:07 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateRoute",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DeleteRoute",
        "ec2:DeleteTags",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkAcls",
```

```
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:RequestSpotInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "elasticmapreduce:*",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListRoles",
        "iam:PassRole",
        "kms:List*",
        "s3:*",
        "sdb:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "elasticmapreduce.amazonaws.com",
            "elasticmapreduce.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack"
```

```
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElasticMapReducePlacementGroupPolicy

Deskripsi: Kebijakan untuk mengizinkan EMR membuat, mendeskripsikan, dan menghapus grup penempatan EC2.

`AmazonElasticMapReducePlacementGroupPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticMapReducePlacementGroupPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 September 2020, 00:37 UTC
- Waktu teredit: 29 September 2020, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Resource" : "*",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeletePlacementGroup",
        "ec2:DescribePlacementGroups"
      ]
    },
    {
      "Resource" : "arn:aws:ec2:*:*:placement-group/EMR_*",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreatePlacementGroup"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElasticMapReduceReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Elastic MapReduce melalui Konsol Manajemen AWS.

`AmazonElasticMapReduceReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticMapReduceReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 29 Juli 2020, 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "sdb:Select",
        "cloudwatch:GetMetricStatistics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElasticMapReduceRole

Deskripsi: Kebijakan ini berada di jalur penghentian. Lihat dokumentasi untuk panduan: Kebijakan https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html. default untuk peran MapReduce layanan Amazon Elastic.

`AmazonElasticMapReduceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticMapReduceRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 24 Juni 2020, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface",
```

```
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:RequestSpotInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DeleteVolume",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfiles",
        "iam:ListRolePolicies",
        "iam:PassRole",
        "s3:CreateBucket",
        "s3:Get*",
        "s3:List*",
        "sdb:BatchPutAttributes",
        "sdb:Select",
        "sqs:CreateQueue",
        "sqs:Delete*",
        "sqs:GetQueue*",
        "sqs:PurgeQueue",
        "sqs:ReceiveMessage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:Describe*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/
AWSServiceRoleForEC2Spot*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElasticsearchServiceRolePolicy

Deskripsi: Izinkan Amazon Elasticsearch Service mengakses AWS layanan lain seperti EC2 Networking API atas nama Anda.

`AmazonElasticsearchServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 07 Juli 2017, 00:15 UTC
- Waktu teredit: 22 Juni 2026, 12:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticsearchServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Stmt1480452973134",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973135",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973136",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/ES"
        }
      }
```

```
    },
    {
      "Sid" : "Stmt1480452973198",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973199",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973200",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973201",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973149",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973150",
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnAssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973194",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973202",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElasticTranscoder_FullAccess

Deskripsi: Memberi pengguna akses penuh ke Elastic Transcoder dan akses ke layanan terkait yang diperlukan untuk fungsionalitas Transcoder Elastic penuh.

`AmazonElasticTranscoder_FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticTranscoder_FullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 April 2018, 18:59 UTC
- Waktu teredit: 10 Juni 2019, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "elastictranscoder.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElasticTranscoder_JobsSubmitter

Deskripsi: Memberi pengguna izin untuk mengubah preset, mengirimkan pekerjaan, dan melihat pengaturan Transcoder Elastic. Kebijakan ini juga memberikan beberapa akses read-only ke

beberapa layanan lain yang diperlukan untuk menggunakan konsol Transcode Elastic, termasuk S3, IAM, dan SNS.

`AmazonElasticTranscoder_JobsSubmitter`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticTranscoder_JobsSubmitter` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Juni 2018, 21:12 UTC
- Waktu teredit: 10 Juni 2019, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "elastictranscoder:*Job",
        "elastictranscoder:*Preset",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
```

```
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElasticTranscoder_ReadOnlyAccess

Deskripsi: Memberi pengguna akses read-only ke Elastic Transcoder dan daftar akses ke layanan terkait.

`AmazonElasticTranscoder_ReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticTranscoder_ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Juni 2018, 21:09 UTC
- Waktu teredit: 10 Juni 2019, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonElasticTranscoderRole

Deskripsi: Kebijakan default untuk peran layanan Transcoder Amazon Elastic.

`AmazonElasticTranscoderRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticTranscoderRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 13 Juni 2019, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:Get*",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:*MultipartUpload*"
      ],
      "Sid" : "1",
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Sid" : "2",
```

```
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEMRCleanupPolicy

Deskripsi: Mengizinkan tindakan yang diperlukan EMR untuk menghentikan dan menghapus sumber daya AWS EC2 jika peran Layanan EMR kehilangan kemampuan tersebut.

`AmazonEMRCleanupPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 26 September 2017, 23:54 UTC
- Waktu teredit: 29 September 2020, 21:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DeleteLaunchTemplate",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances",
        "ec2:CancelSpotInstanceRequests",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume",
        "ec2:DeleteVolume",
        "ec2:DescribePlacementGroups",
        "ec2:DeletePlacementGroup"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEMRContainersServiceRolePolicy

Deskripsi: Mengizinkan akses ke sumber daya AWS layanan lain yang diperlukan untuk menjalankan Amazon EMR

`AmazonEMRContainersServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 09 Desember 2020, 00:38 UTC
- Waktu teredit: 24 Juli 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:ListNodeGroups",
        "eks:DescribeNodeGroup",
        "ec2:DescribeRouteTables",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "eks:ListPodIdentityAssociations",
        "eks:DescribePodIdentityAssociation",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ImportCertificate",
        "acm:AddTagsToCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/emr-container:endpoint:managed-certificate" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:DeleteCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/emr-container:endpoint:managed-certificate" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointServiceCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint-service/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/emr-containers:managed-endpoint-resource" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointServiceManage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpointServiceConfigurations",
        "ec2:ModifyVpcEndpointServicePermissions"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint-service/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/emr-containers:managed-endpoint-resource" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointServiceTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint-service/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpointServiceConfiguration"
        }
      }
    },
    {
      "Sid" : "CloudWatchPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/EMRContainers"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEMRFullAccessPolicy_v2

Deskripsi: Menyediakan akses penuh ke Amazon EMR

`AmazonEMRFullAccessPolicy_v2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEMRFullAccessPolicy_v2` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Maret 2021, 01:50 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RunJobFlowExplicitlyWithEMRManagedTag",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:RunJobFlow"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ElasticMapReduceActions",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:AddInstanceFleet",
        "elasticmapreduce:AddInstanceGroups",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:CancelSteps",
        "elasticmapreduce:CreateEditor",
        "elasticmapreduce:CreatePersistentAppUI",
        "elasticmapreduce:CreateSecurityConfiguration",
        "elasticmapreduce:DeleteEditor",
        "elasticmapreduce:DeleteSecurityConfiguration",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeEditor",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:DescribePersistentAppUI",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeReleaseLabel",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:GetPersistentAppUIPresignedURL",
```

```
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListEditors",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ModifyCluster",
        "elasticmapreduce:ModifyInstanceFleet",
        "elasticmapreduce:ModifyInstanceGroups",
        "elasticmapreduce:OpenEditorInConsole",
        "elasticmapreduce:PutAutoScalingPolicy",
        "elasticmapreduce:PutBlockPublicAccessConfiguration",
        "elasticmapreduce:PutManagedScalingPolicy",
        "elasticmapreduce:RemoveAutoScalingPolicy",
        "elasticmapreduce:RemoveManagedScalingPolicy",
        "elasticmapreduce:RemoveTags",
        "elasticmapreduce:SetTerminationProtection",
        "elasticmapreduce:StartEditor",
        "elasticmapreduce:StopEditor",
        "elasticmapreduce:TerminateJobFlows",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ViewMetricsInEMRConsole",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleForElasticMapReduce",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_DefaultRole_V2",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "elasticmapreduce.amazonaws.com*"
        }
```

```
      }
    },
    {
      "Sid" : "PassRoleForEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "PassRoleForAutoScaling",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "ElasticMapReduceServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticmapreduce.amazonaws.com*/AWSServiceRoleForEMRCleanup*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "elasticmapreduce.amazonaws.com",
            "elasticmapreduce.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleUIActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
```

```
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "s3:ListAllMyBuckets",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEMRReadOnlyAccessPolicy_v2

Deskripsi: Menyediakan akses baca saja ke Amazon EMR dan CloudWatch Metrik terkait.

`AmazonEMRReadOnlyAccessPolicy_v2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEMRReadOnlyAccessPolicy_v2` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Maret 2021, 01:39 UTC

- Waktu teredit: 02 Agustus 2023, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticMapReduceActions",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeEditor",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeReleaseLabel",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListEditors",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "ViewMetricsInEMRConsole",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEMRServerlessServiceRolePolicy

Deskripsi: Mengizinkan akses ke sumber daya AWS layanan lain yang diperlukan untuk menjalankan Amazon EMRServerLess

`AmazonEMRServerlessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 20 Mei 2022, 23:15 UTC
- Waktu teredit: 25 Januari 2024, 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2PolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/EMRServerless",
            "AWS/Usage"
          ]
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEMRServicePolicy_v2

Deskripsi: Kebijakan ini digunakan untuk Peran Layanan Amazon EMR dan TIDAK boleh digunakan untuk pengguna atau peran IAM lainnya di akun Anda. Kebijakan ini memberikan izin untuk membuat dan mengelola sumber daya yang terkait dengan EMR dan layanan terkait yang diperlukan untuk pengoperasian cluster EMR Anda.

`AmazonEMRServicePolicy_v2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEMRServicePolicy_v2` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 12 Maret 2021, 01:11 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateInTaggedNetwork",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateWithEMRTaggedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRTaggedLaunchTemplate",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:CreateLaunchTemplate",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRTaggedInstancesAndVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ResourcesToLaunchEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/ami-*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:ec2:*:*:placement-group/EMR_*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:dedicated-host/*",
        "arn:aws:resource-groups:*:*:group/*"
      ]
```

```
    },
    {
      "Sid" : "ManageEMRTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ManageTagsOnEMRTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterfaceNeededForPrivateSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateTaggedEMRResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateFleet",
            "CreateLaunchTemplate",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "TagPlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:placement-group/EMR_*"
      ]
    },
    {
      "Sid" : "ListActionsForEC2Resources",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDefaultSecurityGroupWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateDefaultSecurityGroupInVPCWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateDefaultSecurityGroupWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid" : "ManageSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRPlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreatePlacementGroup"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:placement-group/EMR_*"
    },
    {
      "Sid" : "DeletePlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeletePlacementGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupsForCapacityReservations",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*_EMR_Auto_Scaling"
    },
    {
      "Sid" : "PassRoleForAutoScaling",
```

```
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "PassRoleForEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "CreateAndModifyEmrServiceVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEmrServiceVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
          "aws:RequestTag/Name" : "emr-service-vpce"
        }
      }
    },
    {
      "Sid" : "TagEmrServiceVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
          "aws:RequestTag/Name" : "emr-service-vpce"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEMRServicePolicyForSessions

Deskripsi: Memberikan izin untuk menyediakan dan mengelola Network Load Balancer, layanan titik akhir VPC, dan grup keamanan yang diperlukan untuk sesi interaktif Amazon EMR Spark Connect di EMR di cluster EC2.

`AmazonEMRServicePolicyForSessions`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEMRServicePolicyForSessions` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 Juni 2026, 19:57 UTC
- Waktu teredit: 22 Juni 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicyForSessions`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NLBProvisioning",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer",
```

```
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*",
        "arn:aws:elasticloadbalancing:*:*:listener/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "NLBManagement",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:SetSecurityGroups",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*",
        "arn:aws:elasticloadbalancing:*:*:listener/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "NLBDescribes",
      "Effect" : "Allow",
```

```
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeListeners",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VPCEndpointServiceProvisioning",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint-service/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointServiceManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpointServiceConfigurations",
        "ec2:ModifyVpcEndpointServicePermissions"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint-service/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointServiceDescribes",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagOnCreateEndpointServiceResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint-service/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpcEndpointServiceConfiguration"
          ]
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRoleForELB",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityGroupProvisioning",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupCreateInVpc",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonESCognitoAccess

Deskripsi: Menyediakan akses terbatas ke layanan konfigurasi Amazon Cognito.

`AmazonESCognitoAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonESCognitoAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Februari 2018, 22:29 UTC
- Waktu teredit: 20 Desember 2021, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESCognitoAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:UpdateUserPoolClient",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:AdminInitiateAuth",
        "cognito-idp:AdminUserGlobalSignOut",
        "cognito-idp:ListUserPoolClients",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:UpdateIdentityPool",
        "cognito-identity:SetIdentityPoolRoles",
        "cognito-identity:GetIdentityPoolRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "cognito-identity.amazonaws.com",
            "cognito-identity-us-gov.amazonaws.com"
          ]
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonESFullAccess

Deskripsi: Menyediakan akses penuh ke layanan konfigurasi Amazon ES.

`AmazonESFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonESFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Oktober 2015, 19:14 UTC
- Waktu teredit: 01 Oktober 2015, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "es:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonESReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke layanan konfigurasi Amazon ES.

`AmazonESReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonESReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Oktober 2015, 19:18 UTC
- Waktu teredit: 03 Oktober 2018, 03:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "es:Describe*",
        "es:List*",
        "es:Get*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEventBridgeApiDestinationsServiceRolePolicy

Deskripsi: Memungkinkan EventBridge untuk mengakses sumber daya Manajer Rahasia atas nama Anda.

`AmazonEventBridgeApiDestinationsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 11 Februari 2021, 20:52 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeApiDestinationsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!connection/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN" : [
            "arn:aws:secretsmanager:*:*:secret:events!connection/*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/EventBridgeApiDestinations" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEventBridgeFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon EventBridge.

`AmazonEventBridgeFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEventBridgeFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Juli 2019, 14:08 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:AWSServiceName" : "apidestinations.events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "schemas.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecretsManagerAccessForApiDestinations",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!*"
    },
    {
      "Sid" : "IAMPassRoleAccessForEventBridge",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForScheduler",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
```

```
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEventBridgePipesFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon P EventBridge ipes.

`AmazonEventBridgePipesFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEventBridgePipesFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2022, 17:03 UTC
- Waktu teredit: 01 Desember 2022, 17.03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgePipesActions",
      "Effect" : "Allow",
      "Action" : "pipes:*",
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEventBridgePipesOperatorAccess

Deskripsi: Menyediakan akses read-only dan operator (kemampuan untuk Menghentikan dan Mulai menjalankan Pipa) ke Amazon EventBridge Pipes.

`AmazonEventBridgePipesOperatorAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEventBridgePipesOperatorAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2022, 17:04 UTC
- Waktu teredit: 01 Desember 2022, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "pipes:StartPipe",
        "pipes:StopPipe"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEventBridgePipesReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke Amazon EventBridge Pipes.

`AmazonEventBridgePipesReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEventBridgePipesReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2022, 17:04 UTC
- Waktu teredit: 01 Desember 2022, 17:04 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEventBridgeReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon EventBridge.

`AmazonEventBridgeReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEventBridgeReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Juli 2019, 13:59 UTC
- Waktu teredit: 24 September 2026, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DescribeEventBus",
        "events:DescribeEventSource",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:TestEventPattern",
        "events:DescribeArchive",
        "events:ListArchives",
        "events:DescribeReplay",
```

```
        "events:ListReplays",
        "events:DescribeConnection",
        "events:ListConnections",
        "events:DescribeApiDestination",
        "events:ListApiDestinations",
        "events:DescribeEndpoint",
        "events:ListEndpoints",
        "events:DescribeSubscriber",
        "events:ListSubscribers",
        "events:GetResourcePolicy",
        "events:ListResourcePolicies",
        "events:ListTagsForResource",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:ExportSchema",
        "schemas:GetCodeBindingSource",
        "schemas:GetDiscoveredSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:ListTagsForResource",
        "schemas:SearchSchemas",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:ListTagsForResource",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEventBridgeSchedulerFullAccess

Deskripsi: Kebijakan AmazonEventBridgeSchedulerFullAccess terkelola memberikan izin untuk menggunakan semua tindakan EventBridge Penjadwal untuk jadwal, dan grup jadwal.

`AmazonEventBridgeSchedulerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEventBridgeSchedulerFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 November 2022, 18:37 UTC
- Waktu teredit: 12 Februari 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : "scheduler:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEventBridgeSchedulerReadOnlyAccess

Deskripsi: Kebijakan AmazonEventBridgeSchedulerReadOnlyAccess terkelola memberikan izin baca-saja untuk melihat detail tentang jadwal dan grup jadwal

`AmazonEventBridgeSchedulerReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEventBridgeSchedulerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 November 2022, 18:50 UTC

- Waktu teredit: 02 April 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "scheduler:List*",
        "scheduler:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEventBridgeSchemasFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon EventBridge Schemas.

`AmazonEventBridgeSchemasFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEventBridgeSchemasFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2019, 23:12 UTC
- Waktu teredit: 28 November 2019, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEventBridgeSchemasFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "schemas:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEventBridgeManageRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
```

```
        "events:PutTargets",
        "events:EnableRule",
        "events:DisableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*Schemas*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEventBridgeSchemasReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon EventBridge Schemas.

`AmazonEventBridgeSchemasReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEventBridgeSchemasReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 28 November 2019, 23:05 UTC
- Waktu teredit: 01 Mei 2020, 00:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEventBridgeSchemasReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "schemas:ListDiscoverers",
        "schemas:DescribeDiscoverer",
        "schemas:ListRegistries",
        "schemas:DescribeRegistry",
        "schemas:SearchSchemas",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:DescribeSchema",
        "schemas:GetDiscoveredSchema",
        "schemas:DescribeCodeBinding",
        "schemas:GetCodeBindingSource",
        "schemas:ListTagsForResource",
        "schemas:GetResourcePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEventBridgeSchemasServiceRolePolicy

Deskripsi: Memberikan izin ke Aturan Terkelola yang dibuat oleh EventBridge skema Amazon.

`AmazonEventBridgeSchemasServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 27 November 2019, 01:10 UTC
- Waktu teredit: 27 November 2019, 01:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:EnableRule",
        "events:DisableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/*Schemas-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonEVSServiceRolePolicy

Deskripsi: Memberikan izin kepada EVS untuk mengelola sumber daya atas nama Anda

`AmazonEVSServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 16 Mei 2025, 23:37 UTC

- Waktu teredit: 22 Maret 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEVSServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "ManageSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSubnet"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "CreateEniWithTagStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "TagOnCreateNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonEVSManaged" : "false"
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "ManageEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
```

```
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ManageInstanceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeInstanceAndVolumeStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageVolumeStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
```

```
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ManageSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "UpdateSecurityGroupStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "CloudWatchPutMetricDataStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Usage",
            "AWS/EVS"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AccessSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/EvsAccess" : "false"
        }
      }
    },
    {
      "Sid" : "DecryptSecretWithKmsKeyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:*:*:secret:*",
          "kms:EncryptionContext:SecretVersionId" : "*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/EvsAccess" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeKmsKeyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
```

```
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/EvsAccess" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonFISServiceRolePolicy

Deskripsi: Kebijakan untuk mengaktifkan AWS FIS mengelola pemantauan dan pemilihan sumber daya untuk eksperimen.

`AmazonFISServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 21 Desember 2020, 21:18 UTC
- Waktu teredit: 25 Oktober 2022, 09:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:DeleteRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "fis.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventBridgeDescribe",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Tagging",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmHistory"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeUserResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "iam:GetUser",
        "iam:GetRole",
        "iam:ListUsers",
        "iam:ListRoles",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "ecs:DescribeClusters",
        "ecs:DescribeTasks",
        "ecs:ListTasks",
        "eks:DescribeNodegroup",
        "eks:DescribeCluster"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonForecastFullAccess

Deskripsi: Memberikan akses ke semua tindakan untuk Amazon Forecast

`AmazonForecastFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonForecastFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Januari 2019, 01:52 UTC
- Waktu teredit: 18 Januari 2019, 01:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonForecastFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "forecast:*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonFraudDetectorFullAccessPolicy

Deskripsi: Memberikan akses ke semua tindakan untuk Amazon Fraud Detector

`AmazonFraudDetectorFullAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonFraudDetectorFullAccessPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 22:46 UTC
- Waktu teredit: 03 Desember 2019, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "frauddetector:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListEndpoints",
        "sagemaker:DescribeEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "frauddetector.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonFreeRTOSFullAccess

Deskripsi: Kebijakan Akses Penuh untuk Amazon FreeRTOS

`AmazonFreeRTOSFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonFreeRTOSFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2017, 15:32 UTC
- Waktu teredit: 29 November 2017, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFreeRTOSFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "freertos:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonFreeRTOSOTAUpdate

Deskripsi: Memungkinkan pengguna untuk mengakses Pembaruan Amazon FreeRTOS OTA

`AmazonFreeRTOSOTAUpdate`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonFreeRTOSOTAUpdate` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 27 Agustus 2018, 22:43 UTC
- Waktu teredit: 18 Desember 2020, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectVersion",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::afr-ota*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "signer:StartSigningJob",
        "signer:DescribeSigningJob",
        "signer:GetSigningProfile",
        "signer:PutSigningProfile"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteJob",
        "iot:DescribeJob"
      ],
      "Resource" : "arn:aws:iot:*:*:job/AFR_OTA*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteStream"
      ],
      "Resource" : "arn:aws:iot:*:*:stream/AFR_OTA*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateStream",
        "iot:CreateJob"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonFSxConsoleFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon FSx dan akses ke AWS layanan terkait melalui. Konsol Manajemen AWS

`AmazonFSxConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonFSxConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2018, 16:36 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v20 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListResourcesAssociatedWithFSxFileSystem",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "ds:DescribeDirectories",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "firehose:ListDeliveryStreams",
        "kms:ListAliases",
        "logs:DescribeLogGroups",
        "s3:ListBucket",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FullAccessToFSx",
      "Effect" : "Allow",
      "Action" : [
        "fsx:AssociateFileGateway",
        "fsx:AssociateFileSystemAliases",
        "fsx:CancelDataRepositoryTask",
        "fsx:CopyBackup",
        "fsx:CopySnapshotAndUpdateVolume",
        "fsx:CreateAndAttachS3AccessPoint",
        "fsx:CreateBackup",
        "fsx:CreateDataRepositoryAssociation",
        "fsx:CreateDataRepositoryTask",
        "fsx:CreateFileCache",
        "fsx:CreateFileSystem",
        "fsx:CreateFileSystemFromBackup",
        "fsx:CreateSnapshot",
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume",
        "fsx:CreateVolumeFromBackup",
        "fsx:DeleteBackup",
        "fsx:DeleteDataRepositoryAssociation",
        "fsx:DeleteFileCache",
        "fsx:DeleteFileSystem",
        "fsx:DeleteSnapshot",
        "fsx:DeleteStorageVirtualMachine",
        "fsx:DeleteVolume",
        "fsx:DescribeAssociatedFileGateways",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeDataRepositoryTasks",
```

```
        "fsx:DescribeFileCaches",
        "fsx:DescribeFileSystemAliases",
        "fsx:DescribeFileSystems",
        "fsx:DescribeS3AccessPointAttachments",
        "fsx:DescribeSharedVpcConfiguration",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:DetachAndDeleteS3AccessPoint",
        "fsx:DisassociateFileGateway",
        "fsx:DisassociateFileSystemAliases",
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:ReleaseFileSystemNfsV3Locks",
        "fsx:RestoreVolumeFromSnapshot",
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx:UpdateDataRepositoryAssociation",
        "fsx:UpdateFileCache",
        "fsx:UpdateFileSystem",
        "fsx:UpdateSharedVpcConfiguration",
        "fsx:UpdateSnapshot",
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateFSxSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateSLRForLustreS3Integration",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "s3.data-source.lustre.fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonFSx" : "ManagedByAmazonFSx"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageCrossAccountDataReplication",
      "Effect" : "Allow",
      "Action" : [
        "fsx:PutResourcePolicy",
        "fsx:GetResourcePolicy",
        "fsx:DeleteResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonFSxConsoleReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon FSx dan akses ke AWS layanan terkait melalui. Konsol Manajemen AWS

`AmazonFSxConsoleReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonFSxConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2018, 16:35 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FSxReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "ds:DescribeDirectories",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "firehose:ListDeliveryStreams",
        "fsx:Describe*",
        "fsx:ListTagsForResource",
        "kms:DescribeKey",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonFSxFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon FSx dan akses ke AWS layanan terkait.

`AmazonFSxFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonFSxFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2018, 16:34 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxFullAccess`

Versi kebijakan

Versi kebijakan: v13 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ViewAWSDSDirectories",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FullAccessToFSx",
```

```
      "Effect" : "Allow",
      "Action" : [
        "fsx:AssociateFileGateway",
        "fsx:AssociateFileSystemAliases",
        "fsx:CancelDataRepositoryTask",
        "fsx:CopyBackup",
        "fsx:CopySnapshotAndUpdateVolume",
        "fsx:CreateAndAttachS3AccessPoint",
        "fsx:CreateBackup",
        "fsx:CreateDataRepositoryAssociation",
        "fsx:CreateDataRepositoryTask",
        "fsx:CreateFileCache",
        "fsx:CreateFileSystem",
        "fsx:CreateFileSystemFromBackup",
        "fsx:CreateSnapshot",
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume",
        "fsx:CreateVolumeFromBackup",
        "fsx:DetachAndDeleteS3AccessPoint",
        "fsx:DeleteBackup",
        "fsx:DeleteDataRepositoryAssociation",
        "fsx:DeleteFileCache",
        "fsx:DeleteFileSystem",
        "fsx:DeleteSnapshot",
        "fsx:DeleteStorageVirtualMachine",
        "fsx:DeleteVolume",
        "fsx:DescribeAssociatedFileGateways",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeDataRepositoryTasks",
        "fsx:DescribeFileCaches",
        "fsx:DescribeFileSystemAliases",
        "fsx:DescribeFileSystems",
        "fsx:DescribeS3AccessPointAttachments",
        "fsx:DescribeSharedVpcConfiguration",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:DisassociateFileGateway",
        "fsx:DisassociateFileSystemAliases",
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:ReleaseFileSystemNfsV3Locks",
        "fsx:RestoreVolumeFromSnapshot",
```

```
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx:UpdateDataRepositoryAssociation",
        "fsx:UpdateFileCache",
        "fsx:UpdateFileSystem",
        "fsx:UpdateSharedVpcConfiguration",
        "fsx:UpdateSnapshot",
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLRForFSx",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateSLRForLustreS3Integration",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "s3.data-source.lustre.fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateLogsForFSxWindowsAuditLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
```

```
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/fsx/*"
      ]
    },
    {
      "Sid" : "WriteToAmazonKinesisDataFirehose",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
      ]
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonFSx" : "ManagedByAmazonFSx"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeEC2VpcResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
```

```
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageCrossAccountDataReplication",
      "Effect" : "Allow",
      "Action" : [
        "fsx:PutResourcePolicy",
        "fsx:GetResourcePolicy",
        "fsx:DeleteResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonFSxReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon FSx.

`AmazonFSxReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonFSxReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2018, 16:33 UTC
- Waktu teredit: 28 November 2018, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:Describe*",
        "fsx:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonFSxServiceRolePolicy

Deskripsi: Mengizinkan Amazon FSx mengelola AWS sumber daya atas nama Anda

`AmazonFSxServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 28 November 2018, 10:38 UTC
- Waktu teredit: 22 Juli 2025, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateFileSystem",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:GetAuthorizedApplicationDetails",
        "ds:UnauthorizeApplication",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAddresses",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:GetSecurityGroupsForVpc",
        "route53:AssociateVPCWithHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PutMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/FSx"
        }
      }
    },
    {
      "Sid" : "TagResourceNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "AmazonFSx.FileSystemId"
        }
      }
    },
    {
      "Sid" : "ManageNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:UnassignIpv6Addresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonFSx.FileSystemId" : "false"
        }
      }
    },
    {
      "Sid" : "ManageRouteTable",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRoute",
        "ec2:ReplaceRoute",
        "ec2:DeleteRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonFSx" : "ManagedByAmazonFSx"
        }
      }
```

```
    },
    {
      "Sid" : "PutCloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/fsx/*"
    },
    {
      "Sid" : "ManageAuditLogs",
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonGlacierFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Glacier melalui Konsol Manajemen AWS.

`AmazonGlacierFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonGlacierFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "glacier:*",
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonGlacierReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Glacier melalui Konsol Manajemen AWS.

`AmazonGlacierReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonGlacierReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 05 Mei 2016, 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "glacier:DescribeJob",
        "glacier:DescribeVault",
        "glacier:GetDataRetrievalPolicy",
        "glacier:GetJobOutput",
        "glacier:GetVaultAccessPolicy",
        "glacier:GetVaultLock",
```

```
        "glacier:GetVaultNotifications",
        "glacier:ListJobs",
        "glacier:ListMultipartUploads",
        "glacier:ListParts",
        "glacier:ListTagsForVault",
        "glacier:ListVaults"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonGrafanaAthenaAccess

Deskripsi: Kebijakan ini memberikan akses ke Amazon Athena dan dependensi yang diperlukan untuk mengaktifkan kueri dan penulisan hasil ke s3 dari plugin Amazon Athena di Amazon Grafana.

`AmazonGrafanaAthenaAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonGrafanaAthenaAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 November 2021, 17:11 UTC
- Waktu teredit: 22 November 2021, 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListTableMetadata",
        "athena:ListWorkGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetWorkGroup",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GrafanaDataSource" : "false"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::grafana-athena-query-results-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonGrafanaCloudWatchAccess

Deskripsi: Kebijakan ini memberikan akses ke Amazon CloudWatch dan dependensi yang diperlukan untuk digunakan CloudWatch sebagai sumber data dalam Amazon Managed Grafana.

`AmazonGrafanaCloudWatchAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonGrafanaCloudWatchAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 24 Maret 2023, 22:41 UTC
- Waktu teredit: 24 Maret 2023, 22:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetInsightRuleReport"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:GetLogGroupFields",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetQueryResults",
        "logs:GetLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:ListSinks",
        "oam:ListAttachedLinks"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonGrafanaRedshiftAccess

Deskripsi: Kebijakan ini memberikan akses cakupan ke Amazon Redshift dan dependensi yang diperlukan untuk menggunakan plugin Amazon Redshift di Amazon Grafana.

`AmazonGrafanaRedshiftAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonGrafanaRedshiftAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 November 2021, 23:15 UTC
- Waktu teredit: 26 November 2021, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:ListTables",
        "redshift-data:ListSchemas"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GrafanaDataSource" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentials",
      "Resource" : [
        "arn:aws:redshift:*:*:dbname:*/*",
        "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "secretsmanager:ResourceTag/RedshiftQueryOwner" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonGrafanaServiceLinkedRolePolicy

Deskripsi: Menyediakan akses ke AWS Sumber Daya yang dikelola atau digunakan oleh Amazon Grafana.

`AmazonGrafanaServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 08 November 2022, 23:10 UTC
- Waktu teredit: 08 November 2022, 23.10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonGrafanaManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
```

```
        },
        "Null" : {
          "aws:RequestTag/AmazonGrafanaManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AmazonGrafanaManaged" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonGuardDutyFullAccess

Deskripsi: Menyediakan akses penuh untuk menggunakan Amazon GuardDuty.

`AmazonGuardDutyFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonGuardDutyFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2017, 22:31 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonGuardDutyFullAccessSid1",
      "Effect" : "Allow",
      "Action" : "guardduty:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleSid1",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ActionsForOrganizationsSid1",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
```

```
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamGetRoleSid1",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
    },
    {
      "Sid" : "AllowPassRoleToMalwareProtection",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "malware-protection-plan.guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonGuardDutyFullAccess_v2

Deskripsi: Menyediakan akses penuh untuk menggunakan Amazon GuardDuty

`AmazonGuardDutyFullAccess_v2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonGuardDutyFullAccess_v2` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Juni 2025, 20:22 UTC
- Waktu teredit: 28 September 2026, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess_v2`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyFullAccess",
      "Effect" : "Allow",
      "Action" : "guardduty:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateGuardDutyServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
```

```
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GuardDutyOrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyOrganizationsAdminAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GuardDutyIamRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
```

```
      "Resource" : "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
    },
    {
      "Sid" : "AllowPassRoleToMalwareProtection",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "malware-protection-plan.guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonGuardDutyMalwareProtectionServiceRolePolicy

Deskripsi: perlindungan GuardDuty malware menggunakan peran terkait layanan (SLR) bernama. AWSServiceRoleForAmazonGuardDutyMalwareProtection Peran terkait layanan ini memungkinkan perlindungan GuardDuty malware untuk melakukan pemindaian tanpa agen untuk mendeteksi malware. Ini memungkinkan GuardDuty untuk membuat snapshot di akun Anda, dan berbagi snapshot dengan akun GuardDuty layanan untuk memindai malware. Ini mengevaluasi snapshot bersama ini dan menyertakan metadata instance EC2 yang diambil dalam temuan Perlindungan GuardDuty Malware. Peran AWSServiceRoleForAmazonGuardDutyMalwareProtection terkait

layanan mempercayai layanan malware-protection.guardduty.amazonaws.com untuk mengambil peran tersebut.

`AmazonGuardDutyMalwareProtectionServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 19 Juli 2022, 19:06 UTC
- Waktu teredit: 25 Januari 2024, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeAndListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ecs:ListClusters",
```

```
        "ecs:ListContainerInstances",
        "ecs:ListTasks",
        "ecs:DescribeTasks",
        "eks:DescribeCluster"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSnapshotVolumeConditionalStatement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotConditionalStatement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyScanId"
        }
      }
    },
    {
      "Sid" : "CreateTagsPermission",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:*/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot"
        }
      }
    },
    {
      "Sid" : "AddTagsToSnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
```

```
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/GuardDutyScanId" : "*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "GuardDutyExcluded",
            "GuardDutyFindingDetected"
          ]
        }
      }
    },
    {
      "Sid" : "DeleteAndShareSnapshotPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/GuardDutyScanId" : "*"
        },
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    },
    {
      "Sid" : "PreventPublicAccessToSnapshotPermission",
      "Effect" : "Deny",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Add/group" : "all"
        }
      }
    },
    {
```

```
      "Sid" : "CreateGrantPermission",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : "snap-*"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "CreateGrant",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo",
            "RetireGrant",
            "DescribeKey"
          ]
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "ShareSnapshotKMSPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "DescribeKeyPermission",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "GuardDutyLogGroupPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/guardduty/*"
    },
    {
      "Sid" : "GuardDutyLogStreamPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/guardduty/*:log-stream:*"
    },
    {
      "Sid" : "EBSDirectAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:GetSnapshotBlock",
        "ebs:ListSnapshotBlocks"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/GuardDutyScanId" : "*"
        },
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonGuardDutyReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke GuardDuty sumber daya Amazon

`AmazonGuardDutyReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonGuardDutyReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2017, 22:29 UTC
- Waktu teredit: 16 November 2023, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:Describe*",
        "guardduty:Get*",
        "guardduty:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonGuardDutyServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Sumber AWS Daya yang digunakan atau dikelola oleh Amazon Guard Duty

`AmazonGuardDutyServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 28 November 2017, 20:12 UTC
- Waktu teredit: 09 September 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v13 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyGetDescribeListPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeTransitGatewayAttachments",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "s3:GetBucketPublicAccessBlock",
```

```
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketTagging",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "eks:ListClusters",
        "eks:DescribeCluster",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ecs:ListClusters",
        "ecs:DescribeClusters",
        "ecs:DescribeTasks",
        "ecs:DescribeTaskDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyCreateSLRPolicy",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateVpcEndpointPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        },
        "StringLike" : {
          "ec2:VpceServiceName" : [
```

```
            "com.amazonaws.*.guardduty-data",
            "com.amazonaws.*.guardduty-data-fips"
          ]
        }
      }
    },
    {
      "Sid" : "GuardDutyModifyDeleteVpcEndpointPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyManaged" : false
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
```

```
        }
      }
    },
    {
      "Sid" : "GuardDutySecurityGroupManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyManaged" : false
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateSecurityGroupPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/GuardDutyManaged" : "*"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateSecurityGroupForVpcPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:CreateAction" : "CreateSecurityGroup"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateEksAddonPolicy",
      "Effect" : "Allow",
      "Action" : "eks:CreateAddon",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyEksAddonManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "eks:DeleteAddon",
        "eks:UpdateAddon",
        "eks:DescribeAddon"
      ],
      "Resource" : "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
    },
    {
      "Sid" : "GuardDutyEksClusterTagResourcePolicy",
      "Effect" : "Allow",
      "Action" : "eks:TagResource",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyEcsPutAccountSettingsDefaultPolicy",
      "Effect" : "Allow",
      "Action" : "ecs:PutAccountSettingDefault",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "ecs:account-setting" : [
            "guardDutyActivate"
          ]
        }
      }
    },
    {
      "Sid" : "SsmCreateDescribeUpdateDeleteStartAssociationPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:DeleteAssociation",
        "ssm:UpdateAssociation",
        "ssm:CreateAssociation",
        "ssm:StartAssociationsOnce"
      ],
      "Resource" : "arn:aws:ssm:*:*:association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/GuardDutyManaged" : "true"
        }
      }
    },
    {
      "Sid" : "SsmAddTagsToResourcePermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:association/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "GuardDutyManaged"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/GuardDutyManaged" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "SsmCreateUpdateAssociationInstanceDocumentPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
    },
    {
      "Sid" : "SsmSendCommandPermission",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin"
      ]
    },
    {
      "Sid" : "SsmGetCommandStatus",
      "Effect" : "Allow",
      "Action" : "ssm:GetCommandInvocation",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudTrailCreateServiceLinkedChannelSid",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/guardduty/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GdLatticeCreateManagedSnvaAssociation",
      "Effect" : "Allow",
      "Action" : "vpc-lattice:CreateServiceNetworkVpcAssociation",
      "Resource" : "arn:aws:vpc-lattice:*:*:servicenetworkvpcassociation/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GdLatticeAssociateViaAwsService",
      "Effect" : "Allow",
      "Action" : "vpc-lattice:AssociateViaAWSService",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonHealthLakeFullAccess

Deskripsi: Menyediakan akses penuh ke HealthLake layanan Amazon.

`AmazonHealthLakeFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonHealthLakeFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Februari 2021, 01:07 UTC
- Waktu teredit: 17 Februari 2021, 01:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "healthlake:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "healthlake.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonHealthLakeReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke HealthLake layanan Amazon.

`AmazonHealthLakeReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonHealthLakeReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Februari 2021, 02:43 UTC
- Waktu teredit: 04 Agustus 2026, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "healthlake:ListFHIRDatastores",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:DescribeFHIRImportJob",
        "healthlake:DescribeFHIRExportJob",
```

```
        "healthlake:GetCapabilities",
        "healthlake:ReadResource",
        "healthlake:SearchWithGet",
        "healthlake:SearchWithPost",
        "healthlake:GetDataTransformationProfile",
        "healthlake:ListDataTransformationProfiles",
        "healthlake:ListDataTransformationProfileVersions",
        "healthlake:DescribeDataTransformationJob",
        "healthlake:ListDataTransformationJobs",
        "healthlake:ValidateSource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonHoneycodeFullAccess

Deskripsi: Menyediakan akses penuh ke Honeycode melalui Konsol Manajemen AWS dan SDK.

`AmazonHoneycodeFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonHoneycodeFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2020, 20:28 UTC
- Waktu teredit: 24 Juni 2020, 20:28 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:*"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonHoneycodeReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Honeycode melalui Konsol Manajemen AWS dan SDK.

`AmazonHoneycodeReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonHoneycodeReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2020, 20:28 UTC
- Waktu teredit: 01 Desember 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:List*",
        "honeycode:Get*",
        "honeycode:Describe*",
        "honeycode:Query*"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonHoneycodeServiceRolePolicy

Deskripsi: Peran terkait layanan yang diperlukan agar Amazon Honeycode dapat mengakses sumber daya Anda.

`AmazonHoneycodeServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 18 November 2020, 18:03 UTC
- Waktu teredit: 18 November 2020, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sso:GetManagedApplicationInstance"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonHoneycodeTeamAssociationFullAccess

Deskripsi: Menyediakan akses penuh ke Asosiasi Tim Honeycode melalui Konsol Manajemen AWS dan SDK.

`AmazonHoneycodeTeamAssociationFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonHoneycodeTeamAssociationFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2020, 20:28 UTC
- Waktu teredit: 24 Juni 2020, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:ListTeamAssociations",
        "honeycode:ApproveTeamAssociation",
        "honeycode:RejectTeamAssociation"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonHoneycodeTeamAssociationReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Asosiasi Tim Honeycode melalui Konsol Manajemen AWS dan SDK.

`AmazonHoneycodeTeamAssociationReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonHoneycodeTeamAssociationReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2020, 20:27 UTC
- Waktu teredit: 24 Juni 2020, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:ListTeamAssociations"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonHoneycodeWorkbookFullAccess

Deskripsi: Menyediakan akses penuh ke Honeycode Workbook melalui Konsol Manajemen AWS dan SDK.

`AmazonHoneycodeWorkbookFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonHoneycodeWorkbookFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2020, 20:28 UTC
- Waktu teredit: 01 Desember 2020, 17:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
```

```
        "honeycode:InvokeScreenAutomation",
        "honeycode:BatchCreateTableRows",
        "honeycode:BatchDeleteTableRows",
        "honeycode:BatchUpdateTableRows",
        "honeycode:BatchUpsertTableRows",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows",
        "honeycode:StartTableDataImportJob"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonHoneycodeWorkbookReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Buku Kerja Honeycode melalui Konsol Manajemen AWS dan SDK.

`AmazonHoneycodeWorkbookReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonHoneycodeWorkbookReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 24 Juni 2020, 20:28 UTC
- Waktu teredit: 01 Desember 2020, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonInspector2AgentlessServiceRolePolicy

Deskripsi: Memberikan akses Amazon Inspector ke Layanan AWS yang diperlukan untuk melakukan penilaian keamanan tanpa agen

`AmazonInspector2AgentlessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 20 November 2023, 15:18 UTC
- Waktu teredit: 20 Agustus 2026, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstanceIdentification",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetSnapshotData",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InspectorScan" : "*"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsAnyInstanceOrVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "DenyCreateSnapshotsOnExcludedInstances",
      "Effect" : "Deny",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/InspectorEc2Exclusion" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsOnAnySnapshotOnlyWithTag",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "InspectorScan"
        }
      }
    },
    {
      "Sid" : "CreateOnlyInspectorScanTagOnlyUsingCreateSnapshots",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:CreateAction" : "CreateSnapshots"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "InspectorScan"
        }
      }
    },
    {
      "Sid" : "DeleteOnlySnapshotsTaggedForScanning",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/InspectorScan" : "*"
        }
      }
    },
    {
      "Sid" : "DenyKmsDecryptForExcludedKeys",
      "Effect" : "Deny",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/InspectorEc2Exclusion" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "DecryptSnapshotBlocksVolContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "vol-*"
        }
      }
    },
    {
      "Sid" : "DecryptSnapshotBlocksSnapContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "snap-*"
        }
      }
    },
    {
      "Sid" : "DescribeKeysForEbsOperations",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "DecryptCrossAccountOrgVolContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "vol-*"
        }
      }
    },
    {
      "Sid" : "DecryptCrossAccountOrgSnapContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "snap-*"
        }
      }
    },
    {
      "Sid" : "DescribeCrossAccountOrgKeysForEbsOperations",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "ListKeyResourceTags",
      "Effect" : "Allow",
      "Action" : "kms:ListResourceTags",
      "Resource" : "arn:aws:kms:*:*:key/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonInspector2AmiScanServiceRolePolicy

Deskripsi: Memberikan akses Amazon Inspector ke yang Layanan AWS diperlukan untuk melakukan penilaian keamanan untuk AMI

`AmazonInspector2AmiScanServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 30 Juli 2026, 17:57 UTC
- Waktu teredit: 30 Juli 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AmiScanServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/DO-NOT-DELETE-AmazonInspector*ManagedRule"
      ]
    },
    {
      "Sid" : "AllowInspectorEnablementForAwsOrgPolicy",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:AssociateMember",
        "inspector2:Disable",
        "inspector2:Enable",
        "inspector2:EnableDelegatedAdminAccount"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowInspectorServiceGetAwsOrg",
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowInspectorServiceDelegatedAdminFromAwsOrg",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "ami.inspector2.amazonaws.com",
            "inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmiIdentification",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetSnapshotData",
      "Effect" : "Allow",
      "Action" : [
        "ebs:GetSnapshotBlock",
        "ebs:ListSnapshotBlocks"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*"
    },
    {
      "Sid" : "DenyGetSnapshotDataOnExcludedSnapshots",
      "Effect" : "Deny",
```

```
      "Action" : [
        "ebs:GetSnapshotBlock",
        "ebs:ListSnapshotBlocks"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/InspectorEc2Exclusion" : "true"
        }
      }
    },
    {
      "Sid" : "DenyKmsDecryptForExcludedKeys",
      "Effect" : "Deny",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/InspectorEc2Exclusion" : "true"
        }
      }
    },
    {
      "Sid" : "DecryptSnapshotBlocksVolContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : "vol-*",
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DecryptSnapshotBlocksSnapContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : "snap-*",
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DescribeKeysForEbsOperations",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListKeyResourceTags",
      "Effect" : "Allow",
      "Action" : "kms:ListResourceTags",
      "Resource" : "arn:aws:kms:*:*:key/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonInspector2FullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Inspector dan akses ke layanan terkait lainnya seperti organisasi.

`AmazonInspector2FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonInspector2FullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2021, 19:10 UTC
- Waktu teredit: 25 April 2024, 13:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFullAccessToInspectorApis",
      "Effect" : "Allow",
      "Action" : "inspector2:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCodeGuruApis",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCreateSlr",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "agentless.inspector2.amazonaws.com",
            "inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonInspector2FullAccess_v2

Deskripsi: Menyediakan akses penuh ke Amazon Inspector dan akses ke layanan terkait lainnya seperti organisasi dengan akses organisasi terbatas.

`AmazonInspector2FullAccess_v2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonInspector2FullAccess_v2` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Juli 2025, 16:07 UTC
- Waktu teredit: 08 Juli 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess_v2`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFullAccessToInspectorApis",
      "Effect" : "Allow",
      "Action" : "inspector2:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCodeGuruApis",
```

```
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCreateSlr",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "agentless.inspector2.amazonaws.com",
            "inspector2.amazonaws.com",
            "thirdparty.inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowServicePrincipalBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "inspector2.amazonaws.com",
            "agentless.inspector2.amazonaws.com",
            "thirdparty.inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOrganizationalBasedAccessToOrganizationApis",
      "Effect" : "Allow",
```

```
      "Action" : [
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "arn:aws:organizations::*:ou/o-*/ou-*"
    },
    {
      "Sid" : "AllowAccountsBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : "arn:aws:organizations::*:account/o-*/*"
    },
    {
      "Sid" : "AllowAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListPoliciesForInspectorPolicyType",
      "Effect" : "Allow",
      "Action" : "organizations:ListPolicies",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
    {
      "Sid" : "AllowDescribeResourcePolicyForDelegation",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeResourcePolicy",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDescribeEffectivePolicyForInspector",
      "Effect" : "Allow",
```

```
      "Action" : "organizations:DescribeEffectivePolicy",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
    {
      "Sid" : "AllowConfigConnectorWriteAndList",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConnector",
        "config:ListConnectors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowConfigConnectorRead",
      "Effect" : "Allow",
      "Action" : "config:GetConnector",
      "Resource" : "arn:aws:config:*:*:connector/*"
    },
    {
      "Sid" : "AllowCreateConfigThirdPartySLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
thirdparty.config.amazonaws.com/AWSServiceRoleForConfigThirdParty",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "thirdparty.config.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonInspector2ManagedCisPolicy

Deskripsi: Ini adalah kebijakan terkelola yang harus dilampirkan pelanggan ke peran mereka untuk berkomunikasi dengan layanan inspektur untuk pemindaian CIS

`AmazonInspector2ManagedCisPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonInspector2ManagedCisPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Januari 2024, 16:31 UTC
- Waktu teredit: 24 Januari 2024, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonInspector2ManagedTelemetryPolicy

Deskripsi: Memberikan izin untuk berkomunikasi dengan Saluran Telemetri Inspector2

`AmazonInspector2ManagedTelemetryPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonInspector2ManagedTelemetryPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 Februari 2026, 17:12 UTC
- Waktu teredit: 13 Februari 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ManagedTelemetryPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForInspector2Telemetry",
      "Effect" : "Allow",
      "Action" : [
        "inspector2-telemetry:StartSession",
        "inspector2-telemetry:StopSession",
        "inspector2-telemetry:SendTelemetry",
        "inspector2-telemetry:NotifyHeartbeat"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonInspector2ReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke layanan Amazon inspector2 dan layanan dukungan yang relevan

`AmazonInspector2ReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonInspector2ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Januari 2022, 14:45 UTC
- Waktu teredit: 07 Juli 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "inspector2:BatchGet*",
        "inspector2:List*",
        "inspector2:Describe*",
        "inspector2:Get*",
        "inspector2:Search*",
```

```
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListPoliciesForInspectorPolicyType",
      "Effect" : "Allow",
      "Action" : "organizations:ListPolicies",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
    {
      "Sid" : "AllowDescribeResourcePolicyForDelegation",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeResourcePolicy",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDescribeEffectivePolicyForInspector",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeEffectivePolicy",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
    {
      "Sid" : "AllowCrossServiceReadsForConnectorHealth",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:ListConfigurationRecorders",
```

```
        "config:GetConnector",
        "config:ListConnectors",
        "ssm:GetCloudConnector",
        "ssm:ListCloudConnectors"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonInspector2ServiceRolePolicy

Deskripsi: Memberikan akses Inspektur Amazon ke Layanan AWS yang diperlukan untuk melakukan penilaian keamanan

`AmazonInspector2ServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 16 November 2021, 20:27 UTC
- Waktu teredit: 16 Juni 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v27 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TirosPolicy",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:DescribeTransitGatewayRouteTables",
```

```
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:GetTransitGatewayPolicyTableAssociations",
        "ec2:GetTransitGatewayPolicyTableEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallMetadata",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "tiros:CreateQuery",
        "tiros:GetQueryAnswer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PackageVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribeImages",
```

```
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:ListImages",
        "ecr:PutRegistryScanningConfiguration",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "ssm:DescribeAssociation",
        "ssm:DescribeAssociationExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:ListAssociations",
        "ssm:ListResourceDataSync"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaPackageVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions",
        "lambda:GetFunction",
        "lambda:GetLayerVersion",
        "lambda:ListTags",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GatherInventory",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:StartAssociationsOnce",
        "ssm:UpdateAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:document/AmazonInspector2-*",
        "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*:*:managed-instance/*",
```

```
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "GatherInventoryDeleteAssociation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "DataSyncCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateResourceDataSync",
        "ssm:DeleteResourceDataSync"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:resource-data-sync/InspectorResourceDataSync-do-not-delete"
      ]
    },
    {
      "Sid" : "ManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/DO-NOT-DELETE-AmazonInspector*ManagedRule"
      ]
    },
    {
      "Sid" : "LambdaCodeVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateScan",
```

```
        "codeguru-security:GetAccountConfiguration",
        "codeguru-security:GetFindings",
        "codeguru-security:GetScan",
        "codeguru-security:ListFindings",
        "codeguru-security:BatchGetFindings",
        "codeguru-security:DeleteScansByCategory"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CodeGuruCodeVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListAttachedRolePolicies",
        "iam:ListPolicies",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "codeguru-security.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "Ec2DeepInspection",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:GetParameters",
        "ssm:DeleteParameter"
      ],
```

```
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/inspector-aws/service/inspector-linux-application-
paths"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowManagementOfServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel"
      ],
      "Resource" : [
        "arn:aws:cloudtrail:*:*:channel/aws-service-channel/inspector2/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListServiceLinkedChannels",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListServiceLinkedChannels"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToRunInvokeCisSpecificDocuments",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AmazonInspector2-InvokeInspectorSsmPluginCIS"
      ]
    },
    {
      "Sid" : "AllowToRunCisCommandsToSpecificResources",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToPutCloudwatchMetricData",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Inspector2"
        }
      }
    },
    {
      "Sid" : "AllowListAccessToECSAndEKS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListClusters",
        "ecs:ListTasks",
```

```
        "eks:ListClusters"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowAccessToECSTasks",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTasks"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowInspectorEnablementForAwsOrgPolicy",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:Enable",
        "inspector2:Disable",
        "inspector2:EnableDelegatedAdminAccount",
        "inspector2:AssociateMember"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowInspectorServiceDelegatedAdminFromAwsOrg",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
```

```
          "organizations:ServicePrincipal" : [
            "agentless.inspector2.amazonaws.com",
            "inspector2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonInspector2ThirdPartyServiceRolePolicy

Deskripsi: Memberikan izin bagi Amazon Inspector untuk melakukan tindakan atas nama Anda untuk pemindaian sumber daya multi-cloud.

`AmazonInspector2ThirdPartyServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 26 Juni 2026, 15:27 UTC
- Waktu teredit: 26 Juni 2026, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ThirdPartyServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MultiCloudResourceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:Search"
      ],
      "Resource" : "arn:aws:resource-explorer-2:*:*:view/ServiceViewForInspector*/
service-view"
    },
    {
      "Sid" : "MultiCloudStreamingAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:CreateStreamingAccessForService",
        "resource-explorer-2:ListStreamingAccessForServices",
        "resource-explorer-2:DeleteStreamingAccessForService"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MultiCloudSsmAssociationWrite",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:StartAssociationsOnce"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-InstallDistributorPackageOnAzure*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
```

```
      "Sid" : "MultiCloudSsmAssociationDescribe",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation"
      ],
      "Resource" : "arn:aws:ssm:*:*:association/*"
    },
    {
      "Sid" : "MultiCloudSsmAssociationList",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListAssociations",
        "ssm:DescribeAssociationExecutions",
        "ssm:DescribeAssociationExecutionTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MultiCloudSsmGetDocument",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AmazonInspector2-*",
        "arn:aws:ssm:*:*:document/AWS-InstallDistributorPackageOnAzure*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MultiCloudSsmAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:GetAutomationExecution",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : [
```

```
        "arn:aws:ssm:*:*:document/AWS-InstallDistributorPackageOnAzure*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ]
    },
    {
      "Sid" : "MultiCloudCloudConnectorManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateCloudConnector",
        "ssm:UpdateCloudConnector",
        "ssm:DeleteCloudConnector",
        "ssm:GetCloudConnector",
        "ssm:ListCloudConnectors",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "ssm:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:cloud-connector/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MultiCloudSsmPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/Inspector2SSMFederationRole*",
        "arn:aws:iam::*:role/Inspector2SSMDispatchRole*",
        "arn:aws:iam::*:role/Inspector2SSMAssumeRole*",
        "arn:aws:iam::*:role/Inspector2VmScannerRole*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "MultiCloudIamGetRole",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
```

```
      "Resource" : [
        "arn:aws:iam::*:role/Inspector2SSMFederationRole*",
        "arn:aws:iam::*:role/Inspector2SSMDispatchRole*",
        "arn:aws:iam::*:role/Inspector2SSMAssumeRole*",
        "arn:aws:iam::*:role/Inspector2VmScannerRole*"
      ]
    },
    {
      "Sid" : "MultiCloudConfigSLRecWrite",
      "Effect" : "Allow",
      "Action" : [
        "config:PutThirdPartyServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:DescribeConfigurationRecorders"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MultiCloudConfigConnectorRead",
      "Effect" : "Allow",
      "Action" : [
        "config:ListConfigurationRecorders",
        "config:GetConnector"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MultiCloudConfigMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetWebIdentityToken",
      "Effect" : "Allow",
      "Action" : "sts:GetWebIdentityToken",
      "Resource" : "*",
```

```
      "Condition" : {
        "Null" : {
          "sts:IdentityTokenAudience" : "false"
        },
        "ForAnyValue:StringLike" : {
          "sts:IdentityTokenAudience" : [
            "api://AzureADTokenExchange"
          ]
        }
      }
    },
    {
      "Sid" : "MultiCloudSsmSLRCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonInspectorFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Inspector.

`AmazonInspectorFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonInspectorFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Oktober 2015, 17:08 UTC
- Waktu teredit: 21 Desember 2017, 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector:*",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "sns:ListTopics",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "inspector.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/inspector.amazonaws.com/
AWSServiceRoleForAmazonInspector",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "inspector.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonInspectorReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Inspector.

`AmazonInspectorReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonInspectorReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Oktober 2015, 17:08 UTC
- Waktu teredit: 01 Oktober 2019, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "sns:ListTopics",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonInspectorServiceRolePolicy

Deskripsi: Memberikan akses Inspektur Amazon ke Layanan AWS yang diperlukan untuk melakukan penilaian keamanan

`AmazonInspectorServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 21 November 2017, 15:48 UTC
- Waktu teredit: 11 September 2020, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "directconnect:DescribeTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:GetTransitGatewayRouteTablePropagations",
```

```
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonKendraFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Kendra melalui. Konsol Manajemen AWS

`AmazonKendraFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKendraFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 16:15 UTC
- Waktu teredit: 03 Desember 2019, 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "kendra.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonKendra-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kendra:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonKendraReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Kendra melalui. Konsol Manajemen AWS

`AmazonKendraReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKendraReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 16:13 UTC
- Waktu teredit: 27 Mei 2021, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kendra:Describe*",
```

```
        "kendra:List*",
        "kendra:Query",
        "kendra:GetQuerySuggestions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonKeyspacesFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Keyspaces

`AmazonKeyspacesFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKeyspacesFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 April 2020, 17:06 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CassandraFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cassandra:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchAlarmsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
```

```
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_CassandraTable",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cassandra.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KeyspacesReplicationServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
replication.cassandra.amazonaws.com/AWSServiceRoleForKeyspacesReplication",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "replication.cassandra.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KeyspacesCDCServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra-
streams.amazonaws.com/AWSServiceRoleForAmazonKeyspacesCDC",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cassandra-streams.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2VpcReadAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonKeyspacesReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Keyspaces

`AmazonKeyspacesReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKeyspacesReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 April 2020, 17:07 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:ListStreams",
        "cassandra:GetStream",
        "cassandra:GetShardIterator",
        "cassandra:GetRecords"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonKeyspacesReadOnlyAccess_v2

Deskripsi: Menyediakan akses baca saja ke Amazon Keyspaces dan AWS layanan terkait.

`AmazonKeyspacesReadOnlyAccess_v2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKeyspacesReadOnlyAccess_v2` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 September 2023, 17:01 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:ListStreams",
```

```
        "cassandra:GetStream",
        "cassandra:GetShardIterator",
        "cassandra:GetRecords"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonKinesisAnalyticsFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Kinesis Analytics melalui. Konsol Manajemen AWS

`AmazonKinesisAnalyticsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKinesisAnalyticsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 September 2016, 19:01 UTC
- Waktu teredit: 21 September 2016, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kinesisanalytics:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:CreateStream",
        "kinesis:DeleteStream",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "kinesis:PutRecord",
```

```
        "kinesis:PutRecords"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:GetLogEvents",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicyVersions",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/kinesis-analytics*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonKinesisAnalyticsReadOnly

Deskripsi: Menyediakan akses baca-saja ke Amazon Kinesis Analytics melalui. Konsol Manajemen AWS

`AmazonKinesisAnalyticsReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKinesisAnalyticsReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 September 2016, 18:16 UTC
- Waktu teredit: 21 September 2016, 18.16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisanalytics:Describe*",
        "kinesisanalytics:Get*",
        "kinesisanalytics:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:GetLogEvents",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicyVersions",
```

```
        "iam:ListRoles"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonKinesisFirehoseFullAccess

Deskripsi: Menyediakan akses penuh ke semua Amazon Kinesis Firehose Delivery Streams.

`AmazonKinesisFirehoseFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKinesisFirehoseFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Oktober 2015, 18:45 UTC
- Waktu teredit: 07 Oktober 2015, 18:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "firehose:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonKinesisFirehoseReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke semua Amazon Kinesis Firehose Delivery Streams.

`AmazonKinesisFirehoseReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKinesisFirehoseReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Oktober 2015, 18:43 UTC
- Waktu teredit: 07 Oktober 2015, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "firehose:Describe*",
        "firehose:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonKinesisFullAccess

Deskripsi: Menyediakan akses penuh ke semua aliran melalui Konsol Manajemen AWS.

`AmazonKinesisFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKinesisFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kinesis:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonKinesisReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke semua aliran melalui Konsol Manajemen AWS.

`AmazonKinesisReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKinesisReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:Get*",
        "kinesis:List*",
        "kinesis:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonKinesisVideoStreamsFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Kinesis Video Streams melalui. Konsol Manajemen AWS

`AmazonKinesisVideoStreamsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKinesisVideoStreamsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2017, 23:27 UTC
- Waktu teredit: 01 Desember 2017, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kinesisvideo:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonKinesisVideoStreamsReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke AWS Kinesis Video Streams melalui. Konsol Manajemen AWS

`AmazonKinesisVideoStreamsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKinesisVideoStreamsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2017, 23:14 UTC
- Waktu teredit: 01 Desember 2017, 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:Describe*",
        "kinesisvideo:Get*",
        "kinesisvideo:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonLaunchWizard_Akses Penuh

Deskripsi: Akses penuh ke Wizard AWS Launch dan layanan lain yang diperlukan.

`AmazonLaunchWizard_Fullaccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLaunchWizard_Fullaccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Agustus 2020, 17:47 UTC
- Waktu teredit: 22 Februari 2023, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-groups:List*",
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets",
        "route53:GetChange",
        "route53:ListResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:List*",
        "cloudwatch:Get*",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateVpc",
```

```
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AllocateHosts",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateVolume",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVolumeAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVolume",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteKeyPair",
        "ec2:DeleteNatGateway",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachVolume",
        "ec2:DeleteSnapshot",
        "ec2:AssociateRouteTable",
        "ec2:AssociateVpcCidrBlock",
```

```
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DetachNetworkInterface",
        "ec2:DisassociateAddress",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:GetLaunchTemplateData",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:GetConsoleOutput",
        "ec2:GetPasswordData",
        "ec2:ReleaseAddress",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:ModifyInstancePlacement",
        "ec2:DeletePlacementGroup",
        "ec2:CreatePlacementGroup",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget",
        "ds:AddIpRoutes",
        "ds:CreateComputer",
        "ds:CreateMicrosoftAD",
        "ds:DeleteDirectory",
        "servicecatalog:AssociateProductWithPortfolio",
        "cloudformation:GetTemplateSummary",
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*",
        "cloudformation:Get*",
        "cloudformation:ListStacks",
        "cloudformation:SignalResource",
        "cloudformation:DeleteStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/LaunchWizard*/*",
        "arn:aws:cloudformation:*:*:stack/ApplicationInsights*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard*",
        "arn:aws:iam::*:role/service-role/AmazonLambdaRoleForLaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "logs:CreateLogStream",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream",
        "logs:DescribeLog*",
        "logs:PutLogEvents",
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "sns:ListSubscriptionsByTopic",
        "sns:Publish",
        "ssm:DeleteDocument",
        "ssm:DeleteParameter*",
        "ssm:DescribeDocument*",
        "ssm:GetDocument",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:resource-groups:*:*:group/LaunchWizard*",
        "arn:aws:sns:*:*:*",
```

```
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
LaunchWizard*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/
LaunchWizard*",
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*",
        "arn:aws:logs:*:*:log-group:*:*:*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunShellScript"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogStream",
        "logs:GetLogEvents",
        "logs:PutLogEvents",
        "ssm:AddTagsToResource",
        "ssm:DescribeDocument",
        "ssm:GetDocument",
```

```
        "ssm:ListTagsForResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*:*:*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*",
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "ds:Describe*",
        "ds:ListAuthorizedApplications",
        "ec2:Describe*",
        "ec2:Get*",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:List*",
        "logs:CreateLogGroup",
        "logs:GetLogDelivery",
        "logs:GetLogRecord",
        "logs:ListLogDeliveries",
        "resource-groups:Get*",
        "resource-groups:List*",
        "servicequotas:GetServiceQuota",
        "servicequotas:ListServiceQuotas",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "ssm:CreateDocument",
        "ssm:DescribeAutomation*",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetCommandInvocation",
```

```
        "ssm:GetParameter*",
        "ssm:GetConnectionStatus",
        "ssm:ListCommand*",
        "ssm:ListDocument*",
        "ssm:ListInstanceAssociations",
        "ssm:SendAutomationSignal",
        "tag:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-definition/LaunchWizard-*:*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:GetLog*",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*:*:*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:List*",
        "cloudformation:Describe*"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/LaunchWizard*/"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "application-insights.amazonaws.com",
            "events.amazonaws.com",
            "autoscaling.amazonaws.com.cn",
            "events.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "launchwizard:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:TagQueue",
        "sqs:GetQueueUrl",
        "sqs:AddPermission",
        "sqs:ListQueues",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : "arn:aws:sqs:*:*:LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "iam:GetInstanceProfile",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:LaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "route53:ListHostedZones",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::launchwizard*",
        "arn:aws:s3:::launchwizard*/*",
        "arn:aws:s3:::aws-sap-data-provider/config.properties"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "LaunchWizard*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketVersioning",
```

```
        "s3:DeleteBucket",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:LaunchWizard*",
        "arn:aws:s3:::launchwizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DescribeTable",
        "dynamodb:DeleteTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsMetadata"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:DeleteOpsMetadata",
      "Resource" : "arn:aws:ssm:*:*:opsmetadata/aws/ssm/LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:UntagResource",
        "fsx:TagResource",
        "fsx:DeleteFileSystem",
        "fsx:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/Name" : "LaunchWizard*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateFileSystem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "aws:RequestTag/Name" : [
            "LaunchWizard*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:CreatePortfolio",
        "servicecatalog:DescribePortfolio",
        "servicecatalog:CreateConstraint",
        "servicecatalog:CreateProduct",
        "servicecatalog:AssociatePrincipalWithPortfolio",
        "servicecatalog:CreateProvisioningArtifact",
        "servicecatalog:TagResource",
        "servicecatalog:UntagResource"
      ],
      "Resource" : [
        "arn:aws:servicecatalog:*:*:*/*",
        "arn:aws:catalog:*:*:*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:UntagResource",
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:TagResource",
        "logs:UntagResource"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:LaunchWizard*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonLaunchWizardFullAccessV2

Deskripsi: Akses penuh ke Wizard AWS Launch dan layanan lain yang diperlukan.

`AmazonLaunchWizardFullAccessV2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLaunchWizardFullAccessV2` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 September 2023, 17:14 UTC
- Waktu teredit: 18 Agustus 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AppInsightsActions0",
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupActions0",
      "Effect" : "Allow",
```

```
      "Action" : "resource-groups:List*",
      "Resource" : "*"
    },
    {
      "Sid" : "Route53Actions0",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets",
        "route53:GetChange",
        "route53:ListResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3Actions0",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsActions0",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchActions0",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:List*",
        "cloudwatch:Get*",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "Ec2Actions0",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateVpc",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2Actions1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AllocateHosts",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVolumeAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVolume",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteKeyPair",
        "ec2:DeleteNatGateway",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachVolume",
        "ec2:DeleteSnapshot",
        "ec2:AssociateRouteTable",
        "ec2:AssociateVpcCidrBlock",
```

```
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DetachNetworkInterface",
        "ec2:DisassociateAddress",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:GetLaunchTemplateData",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVolume",
        "ec2:ReleaseAddress",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:ModifyInstancePlacement",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget",
        "ds:AddIpRoutes",
        "ds:CreateComputer",
        "ds:CreateMicrosoftAD",
        "ds:DeleteDirectory",
        "servicecatalog:AssociateProductWithPortfolio",
        "cloudformation:GetTemplateSummary",
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2InstanceActions0",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
```

```
        "ec2:GetConsoleOutput",
        "ec2:GetPasswordData"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Sid" : "Ec2RunInstancesActions0",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2SecurityGroupActions0",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "Ec2TagActions0",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2VolumeActions0",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2NetworkInterfaceActions0",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2VpcEndpointActions0",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFormationActions0",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*",
        "cloudformation:Get*",
        "cloudformation:ListStacks",
        "cloudformation:SignalResource",
        "cloudformation:DeleteStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/LaunchWizard*/*",
        "arn:aws:cloudformation:*:*:stack/ApplicationInsights*/*"
      ]
```

```
    },
    {
      "Sid" : "CloudFormationActions1",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:List*",
        "cloudformation:Describe*"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/LaunchWizard*/"
    },
    {
      "Sid" : "CloudFormationActions2",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "LaunchWizard*"
        }
      }
    },
    {
      "Sid" : "IamActions0",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ]
    },
    {
      "Sid" : "IamActions1",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard",
        "arn:aws:iam::*:role/service-role/AmazonLambdaRoleForLaunchWizard",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "IamActions2",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "application-insights.amazonaws.com",
            "events.amazonaws.com",
            "autoscaling.amazonaws.com.cn",
            "events.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchWizardActions0",
      "Effect" : "Allow",
      "Action" : "launchwizard:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingActions0",
      "Effect" : "Allow",
      "Action" : [
```

```
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "sns:ListSubscriptionsByTopic",
        "sns:Publish",
        "ssm:DeleteDocument",
        "ssm:DeleteParameter*",
        "ssm:DescribeDocument*",
        "ssm:GetDocument",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:resource-groups:*:*:group/LaunchWizard*",
        "arn:aws:sns:*:*:*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
LaunchWizard*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/
LaunchWizard*",
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*"
      ]
    },
    {
      "Sid" : "SsmActions0",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunShellScript"
      ]
    },
    {
      "Sid" : "SsmActions1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Sid" : "SsmActions2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:DescribeDocument",
        "ssm:GetDocument",
        "ssm:ListTagsForResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*"
      ]
    },
    {
      "Sid" : "SsmActions3",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "ds:Describe*",
        "ds:ListAuthorizedApplications",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeHosts",
        "ec2:DescribeTags",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribePlacementGroups",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:List*",
        "resource-groups:Get*",
        "resource-groups:List*",
        "servicequotas:GetServiceQuota",
        "servicequotas:ListServiceQuotas",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "ssm:CreateDocument",
        "ssm:DescribeAutomation*",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetCommandInvocation",
        "ssm:GetParameter*",
        "ssm:GetConnectionStatus",
```

```
        "ssm:ListCommand*",
        "ssm:ListDocument*",
        "ssm:ListInstanceAssociations",
        "ssm:SendAutomationSignal",
        "tag:Get*",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SsmActions4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-definition/LaunchWizard-*:*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmActions6",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsMetadata",
        "ssm:DeleteOpsMetadata"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsmetadata/aws/ssm/LaunchWizard*"
    },
    {
      "Sid" : "SsmActions7",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SqsActions0",
      "Effect" : "Allow",
      "Action" : [
        "sqs:TagQueue",
        "sqs:GetQueueUrl",
        "sqs:AddPermission",
        "sqs:ListQueues",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : "arn:aws:sqs:*:*:LaunchWizard*"
    },
    {
      "Sid" : "CloudWatchActions1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "iam:GetInstanceProfile",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:LaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ]
    },
    {
      "Sid" : "EfsActions0",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "route53:ListHostedZones",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "elasticfilesystem:DescribeFileSystems",
```

```
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "backup:ListBackupPlans"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EfsCreateActions0",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:CreateMountTarget"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EfsActions1",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:UntagResource",
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3Actions1",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::launchwizard*",
        "arn:aws:s3:::launchwizard*/*",
```

```
        "arn:aws:s3:::aws-sap-data-provider/config.properties"
      ]
    },
    {
      "Sid" : "ElbActions0",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ElbActions1",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:ModifyTargetGroupAttributes",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:RemoveTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "Ec2PlacementGroupActions0",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreatePlacementGroup",
        "ec2:DeletePlacementGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:placement-group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2LaunchTemplateActions0",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:ModifyLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LambdaActions0",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketVersioning",
        "s3:DeleteBucket",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction",
        "lambda:TagResource",
        "lambda:UntagResource"
      ],
      "Resource" : [
```

```
        "arn:aws:lambda:*:*:function:LaunchWizard*",
        "arn:aws:s3:::launchwizard*"
      ]
    },
    {
      "Sid" : "DynamodbActions0",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DescribeTable",
        "dynamodb:DeleteTable",
        "dynamodb:TagResource",
        "dynamodb:UntagResource"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/LaunchWizard*"
    },
    {
      "Sid" : "SecretsManagerActions0",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:LaunchWizard*"
    },
    {
      "Sid" : "SecretsManagerActions1",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsActions0",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:LaunchWizard*"
    },
    {
      "Sid" : "FsxActions0",
      "Effect" : "Allow",
      "Action" : [
        "fsx:UntagResource",
        "fsx:TagResource",
        "fsx:DeleteFileSystem",
        "fsx:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/Name" : "LaunchWizard*"
        }
      }
    },
    {
      "Sid" : "FsxSvmTagActions0",
      "Effect" : "Allow",
      "Action" : [
        "fsx:TagResource",
        "fsx:UntagResource"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:storage-virtual-machine/*/*",
        "arn:aws:fsx:*:*:volume/*/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Sid" : "FsxActions1",
      "Effect" : "Allow",
```

```
      "Action" : [
        "fsx:CreateFileSystem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : [
            "LaunchWizard*"
          ]
        }
      }
    },
    {
      "Sid" : "FsxActions2",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ServiceCatalogActions0",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:CreatePortfolio",
        "servicecatalog:DescribePortfolio",
        "servicecatalog:CreateConstraint",
        "servicecatalog:CreateProduct",
        "servicecatalog:AssociatePrincipalWithPortfolio",
        "servicecatalog:CreateProvisioningArtifact",
        "servicecatalog:TagResource",
        "servicecatalog:UntagResource"
      ],
      "Resource" : [
        "arn:aws:servicecatalog:*:*:*/*",
        "arn:aws:catalog:*:*:*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "LogsActions0",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DeleteLogGroup",
        "logs:DescribeLogStreams",
        "logs:UntagResource",
        "logs:TagResource",
        "logs:CreateLogGroup",
        "logs:DeleteLogStream",
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogDelivery",
        "logs:GetLogGroupFields",
        "logs:GetLogRecord",
        "logs:ListLogDeliveries"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:LaunchWizard*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*:log-stream:*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LogsActions1",
      "Effect" : "Allow",
      "Action" : "logs:DescribeLogGroups",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "FsxActions3",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        },
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Sid" : "FsxActions4",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "FsxActions5",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteStorageVirtualMachine",
        "fsx:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:storage-virtual-machine/*/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        },
        "StringLike" : {
```

```
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonLexChannelsAccess

Deskripsi: Kebijakan ini memungkinkan pelanggan memanggil runtime Lex dari saluran

`AmazonLexChannelsAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 13 Januari 2021, 20:12 UTC
- Waktu teredit: 13 Januari 2021, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexChannelsAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lex:ListBots"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonLexFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Lex melalui Konsol Manajemen AWS. Juga menyediakan akses untuk membuat Lex Service Linked Roles dan memberikan izin Lex untuk memanggil serangkaian fungsi Lambda terbatas.

`AmazonLexFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLexFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 11 April 2017, 23:20 UTC
- Waktu teredit: 16 April 2024, 20:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexFullAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonLexFullAccessStatement1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:GetPolicy",
        "lambda:ListFunctions",
        "lex:*",
        "polly:DescribeVoices",
        "polly:SynthesizeSpeech",
        "kendra:ListIndices",
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "logs:DescribeLogGroups",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "AmazonLexFullAccessStatement2",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AmazonLex*",
      "Condition" : {
        "StringEquals" : {
          "lambda:Principal" : "lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement3",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement4",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : "lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement5",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "channels.lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement6",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lexv2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement7",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "channels.lexv2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement8",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "replication.lexv2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement9",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ]
```

```
    },
    {
      "Sid" : "AmazonLexFullAccessStatement10",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lex.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement11",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lexv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement12",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "channels.lexv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement13",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lexv2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonLexReadOnly

Deskripsi: Menyediakan akses baca-saja ke Amazon Lex.

`AmazonLexReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLexReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 April 2017, 23:13 UTC
- Waktu teredit: 13 Mei 2024, 16:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexReadOnly`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonLexReadOnlyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "lex:GetBot",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "lex:GetBots",
        "lex:GetBotChannelAssociation",
        "lex:GetBotChannelAssociations",
```

```
        "lex:GetBotVersions",
        "lex:GetBuiltinIntent",
        "lex:GetBuiltinIntents",
        "lex:GetBuiltinSlotTypes",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetIntentVersions",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetSlotTypeVersions",
        "lex:GetUtterancesView",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotChannel",
        "lex:DescribeBotLocale",
        "lex:DescribeBotRecommendation",
        "lex:DescribeBotReplica",
        "lex:DescribeBotVersion",
        "lex:DescribeExport",
        "lex:DescribeImport",
        "lex:DescribeIntent",
        "lex:DescribeResourcePolicy",
        "lex:DescribeSlot",
        "lex:DescribeSlotType",
        "lex:ListBots",
        "lex:ListBotLocales",
        "lex:ListBotAliases",
        "lex:ListBotAliasReplicas",
        "lex:ListBotChannels",
        "lex:ListBotRecommendations",
        "lex:ListBotReplicas",
        "lex:ListBotVersions",
        "lex:ListBotVersionReplicas",
        "lex:ListBuiltInIntents",
        "lex:ListBuiltInSlotTypes",
        "lex:ListExports",
        "lex:ListImports",
        "lex:ListIntents",
        "lex:ListRecommendedIntents",
        "lex:ListSlots",
        "lex:ListSlotTypes",
        "lex:ListTagsForResource",
        "lex:SearchAssociatedTranscripts",
        "lex:ListCustomVocabularyItems"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonLexReplicationPolicy

Deskripsi: Mengizinkan Amazon Lex mereplikasi sumber daya Lex di seluruh wilayah atas nama Anda.

`AmazonLexReplicationPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 31 Januari 2024, 23:29 UTC
- Waktu teredit: 24 Juni 2025, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReplicationServicePolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "lex:BuildBotLocale",
        "lex:ListBotLocales",
        "lex:CreateBotAlias",
        "lex:UpdateBotAlias",
        "lex:DeleteBotAlias",
        "lex:DescribeBotAlias",
        "lex:CreateBotVersion",
        "lex:DeleteBotVersion",
        "lex:DescribeBotVersion",
        "lex:CreateExport",
        "lex:DescribeBot",
        "lex:UpdateExport",
        "lex:DescribeExport",
        "lex:DescribeBotLocale",
        "lex:DescribeIntent",
        "lex:ListIntents",
        "lex:DescribeSlotType",
        "lex:ListSlotTypes",
        "lex:DescribeSlot",
        "lex:ListSlots",
        "lex:DescribeCustomVocabulary",
        "lex:StartImport",
        "lex:DescribeImport",
        "lex:CreateBot",
        "lex:UpdateBot",
        "lex:DeleteBot",
        "lex:CreateBotLocale",
        "lex:UpdateBotLocale",
        "lex:DeleteBotLocale",
        "lex:CreateIntent",
```

```
        "lex:UpdateIntent",
        "lex:DeleteIntent",
        "lex:CreateSlotType",
        "lex:UpdateSlotType",
        "lex:DeleteSlotType",
        "lex:CreateSlot",
        "lex:UpdateSlot",
        "lex:DeleteSlot",
        "lex:CreateCustomVocabulary",
        "lex:UpdateCustomVocabulary",
        "lex:DeleteCustomVocabulary",
        "lex:DeleteBotChannel",
        "lex:ListTagsForResource",
        "lex:TagResource",
        "lex:UntagResource",
        "lex:CreateResourcePolicy",
        "lex:DeleteResourcePolicy",
        "lex:DescribeResourcePolicy",
        "lex:UpdateResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:lex:*:*:bot/*",
        "arn:aws:lex:*:*:bot-alias/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReplicationServicePolicyStatement2",
      "Effect" : "Allow",
      "Action" : [
        "lex:CreateUploadUrl",
        "lex:ListBots"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "ReplicationServicePolicyStatement3",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lexv2.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonLexRunBotsOnly

Deskripsi: Menyediakan akses ke API percakapan Amazon Lex.

`AmazonLexRunBotsOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLexRunBotsOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 April 2017, 23:06 UTC
- Waktu teredit: 18 Agustus 2021, 00:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexRunBotsOnly`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lex:PostContent",
        "lex:PostText",
        "lex:PutSession",
        "lex:GetSession",
        "lex:DeleteSession",
        "lex:RecognizeText",
        "lex:RecognizeUtterance",
        "lex:StartConversation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonLexV2BotPolicy

Deskripsi: Menyediakan akses bot Lex V2 untuk memang AWS gil layanan lain atas nama Anda.

`AmazonLexV2BotPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 13 Januari 2021, 20:10 UTC
- Waktu teredit: 13 Januari 2021, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonLookoutEquipmentFullAccess

Deskripsi: Menyediakan akses penuh ke operasi Amazon Lookout for Equipment

`AmazonLookoutEquipmentFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLookoutEquipmentFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 April 2021, 15:52 UTC
- Waktu teredit: 24 November 2021, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "lookoutequipment:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lookoutequipment.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "lookoutequipment.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonLookoutEquipmentReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Lookout untuk Peralatan

`AmazonLookoutEquipmentReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLookoutEquipmentReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Mei 2021, 16:47 UTC
- Waktu teredit: 10 November 2022, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutequipment:Describe*",
        "lookoutequipment:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonLookoutMetricsFullAccess

Deskripsi: Memberikan akses ke semua tindakan untuk Amazon Lookout for Metrics

`AmazonLookoutMetricsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLookoutMetricsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Mei 2021, 00:43 UTC
- Waktu teredit: 07 Mei 2021, 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutmetrics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*LookoutMetrics*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lookoutmetrics.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonLookoutMetricsReadOnlyAccess

Deskripsi: Memberikan akses ke semua tindakan baca-saja untuk Amazon Lookout for Metrics

`AmazonLookoutMetricsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLookoutMetricsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Mei 2021, 00:43 UTC
- Waktu teredit: 04 Januari 2022 18.19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutmetrics:DescribeMetricSet",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:DescribeAnomalyDetectionExecutions",
        "lookoutmetrics:DescribeAlert",
```

```
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListTagsForResource",
        "lookoutmetrics:ListAnomalyGroupSummaries",
        "lookoutmetrics:ListAnomalyGroupTimeSeries",
        "lookoutmetrics:ListAnomalyGroupRelatedMetrics",
        "lookoutmetrics:GetAnomalyGroup",
        "lookoutmetrics:GetDataQualityMetrics",
        "lookoutmetrics:GetSampleData",
        "lookoutmetrics:GetFeedback"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonLookoutVisionConsoleFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Lookout for Vision dan akses cakupan ke dependensi layanan dan konsol yang diperlukan.

`AmazonLookoutVisionConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLookoutVisionConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Mei 2021, 19:37 UTC
- Waktu teredit: 11 Mei 2021, 19:37 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketSearchAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketFirstUseSetupAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*"
```

```
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketVersioning"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*/*"
    },
    {
      "Sid" : "LookoutVisionConsoleDatasetLabelingToolsAccess",
      "Effect" : "Allow",
      "Action" : [
        "groundtruthlabeling:RunGenerateManifestByCrawlingJob",
        "groundtruthlabeling:AssociatePatchToManifestJob",
        "groundtruthlabeling:DescribeConsoleJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleTagSelectorAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleKmsKeySelectorAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonLookoutVisionConsoleReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Lookout for Vision dan akses cakupan ke dependensi layanan dan konsol yang diperlukan.

`AmazonLookoutVisionConsoleReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLookoutVisionConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 11 Mei 2021, 19:32 UTC
- Waktu teredit: 09 Desember 2021, 02:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeProject",
        "lookoutvision:DescribeTrialDetection",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "lookoutvision:ListTrialDetections",
        "lookoutvision:ListModelPackagingJobs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketSearchAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3ObjectReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*/*"
    },
    {
      "Sid" : "LookoutVisionConsoleDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonLookoutVisionFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Lookout for Vision dan akses cakupan ke dependensi yang diperlukan.

`AmazonLookoutVisionFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLookoutVisionFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Mei 2021, 19:24 UTC
- Waktu teredit: 11 Mei 2021 19.24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonLookoutVisionReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Lookout for Vision dan akses cakupan ke dependensi yang diperlukan.

`AmazonLookoutVisionReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLookoutVisionReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Mei 2021, 19:11 UTC
- Waktu teredit: 09 Desember 2021, 03:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "LookoutVisionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeProject",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "lookoutvision:ListModelPackagingJobs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMachineLearningBatchPredictionsAccess

Deskripsi: Memberikan izin kepada pengguna untuk meminta prediksi batch Amazon Machine Learning.

`AmazonMachineLearningBatchPredictionsAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMachineLearningBatchPredictionsAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 09 April 2015, 17:12 UTC
- Waktu teredit: 09 April 2015, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning:DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
        "machinelearning:UpdateBatchPrediction"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMachineLearningCreateOnlyAccess

Deskripsi: Menyediakan akses buat untuk sumber daya Amazon Machine Learning non-prediksi.

`AmazonMachineLearningCreateOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMachineLearningCreateOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 April 2015, 17:18 UTC
- Waktu teredit: 29 Juni 2016, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning:Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMachineLearningFullAccess

Deskripsi: Menyediakan akses penuh ke sumber daya Amazon Machine Learning.

`AmazonMachineLearningFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMachineLearningFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 April 2015, 17:25 UTC
- Waktu teredit: 09 April 2015, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

Deskripsi: Memberikan izin kepada pengguna untuk membuat dan menghapus titik akhir waktu nyata untuk model Amazon Machine Learning.

`AmazonMachineLearningManageRealTimeEndpointOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMachineLearningManageRealTimeEndpointOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 April 2015, 17:32 UTC

- Waktu teredit: 09 April 2015, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningManageRealTimeEndpointOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateRealtimeEndpoint",
        "machinelearning:DeleteRealtimeEndpoint"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMachineLearningReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke sumber daya Amazon Machine Learning.

`AmazonMachineLearningReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMachineLearningReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 April 2015, 17:40 UTC
- Waktu teredit: 09 April 2015, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMachineLearningRealTimePredictionOnlyAccess

Deskripsi: Memberikan izin kepada pengguna untuk meminta prediksi real-time Amazon Machine Learning.

`AmazonMachineLearningRealTimePredictionOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMachineLearningRealTimePredictionOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 April 2015, 17:44 UTC
- Waktu teredit: 09 April 2015, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningRealTimePredictionOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Predict"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMachineLearningRoleforRedshiftDataSourceV3

Deskripsi: Memungkinkan Pembelajaran Mesin untuk mengonfigurasi dan menggunakan Cluster Redshift dan Lokasi Pementasan S3 untuk Sumber Data Pergeseran Merah.

`AmazonMachineLearningRoleforRedshiftDataSourceV3`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMachineLearningRoleforRedshiftDataSourceV3` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 24 Juni 2020, 18:00 UTC
- Waktu teredit: 24 Juni 2020, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupIngress",
        "redshift:AuthorizeClusterSecurityGroupIngress",
        "redshift:CreateClusterSecurityGroup",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:ModifyCluster",
        "redshift:RevokeClusterSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketLocation",
```

```
        "s3:GetBucketPolicy",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::amazon-machine-learning*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMacieFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Macie.

`AmazonMacieFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMacieFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Agustus 2017, 14:54 UTC
- Waktu teredit: 01 Juli 2022, 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "pricing:GetProducts",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMacieHandshakeRole

Deskripsi: Memberikan izin untuk membuat peran terkait layanan Amazon Macie.

`AmazonMacieHandshakeRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMacieHandshakeRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 28 Juni 2018, 15:46 UTC
- Waktu teredit: 28 Juni 2018, 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMacieReadOnlyAccess

Deskripsi: Menyediakan akses readonly ke Amazon Macie.

`AmazonMacieReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMacieReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Juni 2023, 21:50 UTC
- Waktu teredit: 15 Juni 2023, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:SearchResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMacieServiceRole

Deskripsi: Memberikan Macie akses baca-saja ke dependensi sumber daya di akun Anda untuk mengaktifkan analisis data.

`AmazonMacieServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMacieServiceRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Agustus 2017, 14:53 UTC
- Waktu teredit: 14 Agustus 2017, 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMacieServiceRolePolicy

Deskripsi: Peran terkait layanan untuk Amazon Macie

`AmazonMacieServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 19 Juni 2018, 22:17 UTC
- Waktu teredit: 19 Mei 2022 19.16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMacieServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccountAliases",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
```

```
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/macie/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/macie/*:log-stream:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonManagedBlockchainConsoleFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Managed Blockchain melalui Konsol Manajemen AWS

`AmazonManagedBlockchainConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonManagedBlockchainConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 April 2019, 21:23 UTC
- Waktu teredit: 29 April 2019, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:*",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonManagedBlockchainFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Managed Blockchain.

`AmazonManagedBlockchainFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonManagedBlockchainFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 April 2019, 21:39 UTC

- Waktu teredit: 29 April 2019, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonManagedBlockchainReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke Amazon Managed Blockchain.

`AmazonManagedBlockchainReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonManagedBlockchainReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 April 2019, 18:17 UTC
- Waktu teredit: 30 April 2019, 18.17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:Get*",
        "managedblockchain:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonManagedBlockchainServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Amazon Managed Blockchain

`AmazonManagedBlockchainServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 17 Januari 2020, 19:51 UTC
- Waktu teredit: 17 Januari 2020, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/managedblockchain/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/managedblockchain/*:log-stream:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMCSFullAccess

Deskripsi: Menyediakan akses penuh ke Layanan Apache Cassandra yang Dikelola Amazon

`AmazonMCSFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMCSFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 13:45 UTC
- Waktu teredit: 17 April 2020, 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DescribeScheduledActions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:*"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_CassandraTable",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cassandra.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMCSReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Layanan Apache Cassandra yang Dikelola Amazon

`AmazonMCSReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMCSReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 13:46 UTC
- Waktu teredit: 17 April 2020, 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMechanicalTurkFullAccess

Deskripsi: Menyediakan akses penuh ke semua API di Amazon Mechanical Turk.

`AmazonMechanicalTurkFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMechanicalTurkFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Desember 2015, 19:08 UTC
- Waktu teredit: 11 Desember 2015, 19:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mechanicalturk:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMechanicalTurkReadOnly

Deskripsi: Menyediakan akses ke API hanya baca di Amazon Mechanical Turk.

`AmazonMechanicalTurkReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMechanicalTurkReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Desember 2015, 19:08 UTC
- Waktu teredit: 25 September 2019, 21:06 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkReadOnly`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mechanicalturk:Get*",
        "mechanicalturk:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMemoryDBFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon MemoryDB melalui. Konsol Manajemen AWS

`AmazonMemoryDBFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMemoryDBFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Oktober 2021, 19:24 UTC
- Waktu teredit: 08 Oktober 2021 19.24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "memorydb:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/memorydb.amazonaws.com/
AWSServiceRoleForMemoryDB",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "memorydb.amazonaws.com"
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMemoryDBReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon MemoryDB melalui. Konsol Manajemen AWS

`AmazonMemoryDBReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMemoryDBReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Oktober 2021, 19:27 UTC
- Waktu teredit: 08 Oktober 2021 19.27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "memorydb:Describe*",
        "memorydb:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMobileAnalyticsFinancialReportAccess

Deskripsi: Menyediakan akses baca saja ke semua laporan termasuk data keuangan untuk semua sumber daya aplikasi.

`AmazonMobileAnalyticsFinancialReportAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMobileAnalyticsFinancialReportAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFinancialReportAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mobileanalytics:GetReports",
        "mobileanalytics:GetFinancialReports"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMobileAnalyticsFullAccess

Deskripsi: Menyediakan akses penuh ke semua sumber daya aplikasi.

`AmazonMobileAnalyticsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMobileAnalyticsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mobileanalytics:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMobileAnalyticsNon-financialReportAccess

Deskripsi: Menyediakan akses baca saja ke laporan non keuangan untuk semua sumber daya aplikasi.

`AmazonMobileAnalyticsNon-financialReportAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMobileAnalyticsNon-financialReportAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : "mobileanalytics:GetReports",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMobileAnalyticsWriteOnlyAccess

Deskripsi: Menyediakan akses menulis saja untuk menempatkan data peristiwa untuk semua sumber daya aplikasi. (Direkomendasikan untuk integrasi SDK)

`AmazonMobileAnalyticsWriteOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMobileAnalyticsWriteOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mobileanalytics:PutEvents",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMonitronFullAccess

Deskripsi: Menyediakan akses penuh untuk mengelola Amazon Monitron

`AmazonMonitronFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMonitronFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Desember 2020, 22:40 UTC
- Waktu teredit: 08 Juni 2022, 16:27 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonMonitronFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "monitron.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "monitron:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "monitron.*.amazonaws.com"
          ]
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Sid" : "AWSSSOPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "ds:DescribeDirectories",
        "ds:DescribeTrusts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/monitron/*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMQApiFullAccess

Deskripsi: Menyediakan akses penuh ke AmazonMQ melalui kami. API/SDK

`AmazonMQApiFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMQApiFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Desember 2018, 20:31 UTC
- Waktu teredit: 04 November 2020, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mq:*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
      ]
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "mq.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMQApiReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke AmazonMQ melalui kami. API/SDK

`AmazonMQApiReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMQApiReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Desember 2018, 20:31 UTC
- Waktu teredit: 18 Desember 2018, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMQFullAccess

Deskripsi: Menyediakan akses penuh ke AmazonMQ melalui. Konsol Manajemen AWS

`AmazonMQFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMQFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2017, 15:28 UTC

- Waktu teredit: 03 September 2026, 22:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mq:*",
        "cloudformation:CreateStack",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/mq.amazonaws.com/
AWSServiceRoleForAmazonMQ",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "mq.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMQReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke AmazonMQ melalui. Konsol Manajemen AWS

`AmazonMQReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMQReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2017, 15:30 UTC
- Waktu teredit: 28 November 2017, 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMQServiceRolePolicy

Deskripsi: Kebijakan Peran Terkait Layanan untuk AWS Amazon MQ

`AmazonMQServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 04 November 2020, 16:07 UTC
- Waktu teredit: 04 November 2020, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AMQManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AMQManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMSKConnectReadOnlyAccess

Deskripsi: Menyediakan akses readonly ke Amazon MSK Connect

`AmazonMSKConnectReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMSKConnectReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 September 2021, 10:18 UTC
- Waktu teredit: 18 Oktober 2021, 09:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListWorkerConfigurations"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:DescribeConnector"
      ],
      "Resource" : [
        "arn:aws:kafkaconnect:*:*:connector/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:DescribeCustomPlugin"
      ],
      "Resource" : [
        "arn:aws:kafkaconnect:*:*:custom-plugin/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:DescribeWorkerConfiguration"
      ],
      "Resource" : [
        "arn:aws:kafkaconnect:*:*:worker-configuration/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMSKFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon MSK dan izin lain yang diperlukan untuk dependensinya.

`AmazonMSKFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMSKFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Januari 2019, 22:07 UTC
- Waktu teredit: 18 Oktober 2023, 11:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:*",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints",
```

```
        "ec2:DescribeVpcAttribute",
        "kms:DescribeKey",
        "kms:CreateGrant",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "S3:GetBucketPolicy",
        "firehose:TagDeliveryStream"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc/*",
        "arn:*:ec2:*:*:subnet/*",
        "arn:*:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
          "aws:RequestTag/ClusterArn" : "*"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
          "ec2:ResourceTag/ClusterArn" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "kafka.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/kafka.amazonaws.com/
AWSServiceRoleForKafka*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:AWSServiceName" : "kafka.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "delivery.logs.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMSKReadOnlyAccess

Deskripsi: Menyediakan akses readonly ke Amazon MSK

`AmazonMSKReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMSKReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Januari 2019, 22:28 UTC

- Waktu teredit: 14 Januari 2019, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "kafka:Describe*",
        "kafka:List*",
        "kafka:Get*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMWAAServerlessServiceRolePolicy

Deskripsi: Menyediakan akses ke Amazon Airflow Serverless Service untuk mengelola jaringan alur kerja Anda dan mengakses AWS layanan lain atas nama Anda

`AmazonMWAAServerlessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 15 November 2025, 20:34 UTC
- Waktu teredit: 15 November 2025, 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServerlessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
```

```
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonMWAAServiceRolePolicy

Deskripsi: Peran Tertaut Layanan yang digunakan oleh Alur Kerja Terkelola Amazon untuk Apache Airflow.

`AmazonMWAAServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 24 November 2020, 14:13 UTC
- Waktu teredit: 17 November 2022, 00:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:airflow-*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
```

```
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "AmazonMWAAManaged"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonMWAAManaged" : false
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "AmazonMWAAManaged"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/MWAA"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonNimbleStudio-LaunchProfileWorker

Deskripsi: Kebijakan ini memberikan akses ke sumber daya yang dibutuhkan oleh pekerja Profil Peluncuran Nimble Studio. Lampirkan kebijakan ini ke instans EC2 yang dibuat oleh Nimble Studio Builder.

`AmazonNimbleStudio-LaunchProfileWorker`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonNimbleStudio-LaunchProfileWorker` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 April 2021, 04:47 UTC
- Waktu teredit: 28 April 2021, 04:47 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "nimble.amazonaws.com"
        }
      },
      "Sid" : "GetLaunchProfileInitializationDependencies"
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonNimbleStudio-StudioAdmin

Deskripsi: Kebijakan ini memberikan akses ke sumber daya Amazon Nimble Studio yang terkait dengan admin studio dan sumber daya studio terkait di layanan lain. Lampirkan kebijakan ini ke peran Admin yang terkait dengan studio Anda.

`AmazonNimbleStudio-StudioAdmin`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonNimbleStudio-StudioAdmin` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 April 2021, 04:47 UTC
- Waktu teredit: 22 September 2023, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Sid" : "StudioAdminFullAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "nimble:CreateStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:DeleteStreamingSession",
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetEula",
        "nimble:AcceptEulas",
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListStreamingSessions",
        "nimble:GetStreamingImage",
        "nimble:ListStreamingImages",
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents",
        "nimble:ListLaunchProfiles",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileMember",
        "nimble:ListLaunchProfileMembers",
        "nimble:PutLaunchProfileMembers",
        "nimble:UpdateLaunchProfileMember",
        "nimble:DeleteLaunchProfileMember"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ds:DescribeDirectories",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "nimble.amazonaws.com"
        }
      }
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonNimbleStudio-StudioUser

Deskripsi: Kebijakan ini memberikan akses ke sumber daya Amazon Nimble Studio yang terkait dengan pengguna studio dan sumber daya studio terkait di layanan lain. Lampirkan kebijakan ini ke peran Pengguna yang terkait dengan studio Anda.

`AmazonNimbleStudio-StudioUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonNimbleStudio-StudioUser` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 April 2021, 04:48 UTC
- Waktu teredit: 22 September 2023, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
```

```
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "nimble.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "nimble:ListLaunchProfiles"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "nimble:requesterPrincipalId" : "${nimble:principalId}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "nimble:DeleteStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:ListStreamingSessions",
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "nimble:ownedBy" : "${nimble:requesterPrincipalId}"
        }
      }
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonODBAutonomousDatabaseAdmin

Deskripsi: Menyediakan akses administratif untuk mengelola sumber daya Database Otonom di Oracle Database@AWS.

`AmazonODBAutonomousDatabaseAdmin`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonODBAutonomousDatabaseAdmin` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan fungsi pekerjaan
- Waktu pembuatan: 04 September 2026, 21:47 UTC
- Waktu teredit: 04 September 2026, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AmazonODBAutonomousDatabaseAdmin`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowODBActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:GetOciOnboardingStatus",
        "odb:InitializeService",
        "odb:CreateAutonomousDatabase",
        "odb:GetAutonomousDatabase",
        "odb:UpdateAutonomousDatabase",
        "odb:DeleteAutonomousDatabase",
        "odb:ListAutonomousDatabases",
        "odb:ListAutonomousDatabaseClones",
        "odb:ListAutonomousDatabasePeers",
        "odb:StartAutonomousDatabase",
```

```
        "odb:StopAutonomousDatabase",
        "odb:RebootAutonomousDatabase",
        "odb:ShrinkAutonomousDatabase",
        "odb:SwitchoverAutonomousDatabase",
        "odb:FailoverAutonomousDatabase",
        "odb:RestoreAutonomousDatabase",
        "odb:CreateAutonomousDatabaseWallet",
        "odb:GetAutonomousDatabaseWalletDetails",
        "odb:CreateAutonomousDatabaseBackup",
        "odb:GetAutonomousDatabaseBackup",
        "odb:UpdateAutonomousDatabaseBackup",
        "odb:DeleteAutonomousDatabaseBackup",
        "odb:ListAutonomousDatabaseBackups",
        "odb:GetOdbNetwork",
        "odb:ListOdbNetworks",
        "odb:ListAutonomousDatabaseVersions",
        "odb:ListAutonomousDatabaseCharacterSets",
        "odb:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSLRActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "odb.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "AllowTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:TagResource",
        "odb:UntagResource"
      ],
      "Resource" : [
        "arn:aws:odb:*:*:autonomous-database/*",
        "arn:aws:odb:*:*:autonomous-database-backup/*"
      ]
    },
    {
      "Sid" : "AllowOutboundIntegrationActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:CreateOutboundIntegration",
        "odb:UpdateOutboundIntegration"
      ],
      "Resource" : [
        "arn:aws:odb:*:*:autonomous-database/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonODBAutonomousVmClusterAdmin

Deskripsi: Menyediakan akses administratif untuk mengelola sumber daya cluster VM Autonomous di Oracle Database@AWS

`AmazonODBAutonomousVmClusterAdmin`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonODBAutonomousVmClusterAdmin` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan fungsi pekerjaan
- Waktu pembuatan: 07 Agustus 2026, 01:12 UTC
- Waktu teredit: 04 September 2026, 21:17 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AmazonODBAutonomousVmClusterAdmin`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowODBActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:GetOciOnboardingStatus",
        "odb:InitializeService",
        "odb:GetCloudExadataInfrastructure",
        "odb:GetCloudExadataInfrastructureUnallocatedResources",
        "odb:ListCloudExadataInfrastructures",
        "odb:CreateCloudAutonomousVmCluster",
        "odb:GetCloudAutonomousVmCluster",
        "odb:DeleteCloudAutonomousVmCluster",
        "odb:ListCloudAutonomousVmClusters",
        "odb:AssociateIamRoleToResource",
```

```
        "odb:DisassociateIamRoleFromResource",
        "odb:ListDbServers",
        "odb:GetOdbNetwork",
        "odb:ListOdbNetworks",
        "odb:ListAutonomousVirtualMachines",
        "odb:ListDbSystemShapes",
        "odb:ListGiVersions",
        "odb:ListSystemVersions",
        "odb:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:TagResource",
        "odb:UntagResource"
      ],
      "Resource" : [
        "arn:aws:odb:*:*:cloud-autonomous-vm-cluster/*"
      ]
    },
    {
      "Sid" : "AllowOutboundIntegrationActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:CreateOutboundIntegration",
        "odb:UpdateOutboundIntegration"
      ],
      "Resource" : [
        "arn:aws:odb:*:*:cloud-autonomous-vm-cluster/*"
      ]
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonODBExadataInfrastructureAdmin

Deskripsi: Menyediakan akses administratif untuk mengelola sumber daya Exadata Infrastructure di Oracle Database@AWS

`AmazonODBExadataInfrastructureAdmin`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonODBExadataInfrastructureAdmin` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan fungsi pekerjaan
- Waktu pembuatan: 07 Agustus 2026, 01:12 UTC
- Waktu teredit: 04 September 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AmazonODBExadataInfrastructureAdmin`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowODBActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:GetOciOnboardingStatus",
        "odb:InitializeService",
        "odb:CreateCloudExadataInfrastructure",
        "odb:GetCloudExadataInfrastructure",
        "odb:UpdateCloudExadataInfrastructure",
        "odb:GetCloudExadataInfrastructureUnallocatedResources",
        "odb:DeleteCloudExadataInfrastructure",
        "odb:ListCloudExadataInfrastructures",
        "odb:ListCloudVmClusters",
        "odb:ListCloudAutonomousVmClusters",
        "odb:GetDbServer",
        "odb:ListDbServers",
        "odb:ListDbSystemShapes",
        "odb:ListFlexComponents",
        "odb:PutResourcePolicy",
        "odb:GetResourcePolicy",
        "odb:DeleteResourcePolicy",
        "odb:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSLRActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "odb.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:TagResource",
        "odb:UntagResource"
      ],
      "Resource" : [
        "arn:aws:odb:*:*:cloud-exadata-infrastructure/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonODBExadataVmClusterAdmin

Deskripsi: Menyediakan akses administratif untuk mengelola sumber daya cluster Exadata VM di Oracle Database@.AWS

`AmazonODBExadataVmClusterAdmin`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonODBExadataVmClusterAdmin` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan fungsi pekerjaan
- Waktu pembuatan: 04 September 2026, 21:37 UTC
- Waktu teredit: 04 September 2026, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AmazonODBExadataVmClusterAdmin`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowODBActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:GetOciOnboardingStatus",
        "odb:InitializeService",
        "odb:GetCloudExadataInfrastructure",
        "odb:GetCloudExadataInfrastructureUnallocatedResources",
        "odb:ListCloudExadataInfrastructures",
        "odb:CreateCloudVmCluster",
        "odb:GetCloudVmCluster",
        "odb:DeleteCloudVmCluster",
        "odb:ListCloudVmClusters",
        "odb:AssociateIamRoleToResource",
        "odb:DisassociateIamRoleFromResource",
```

```
        "odb:CreateDbNode",
        "odb:GetDbNode",
        "odb:RebootDbNode",
        "odb:StartDbNode",
        "odb:StopDbNode",
        "odb:DeleteDbNode",
        "odb:ListDbNodes",
        "odb:GetDbServer",
        "odb:ListDbServers",
        "odb:GetOdbNetwork",
        "odb:ListOdbNetworks",
        "odb:ListDbSystemShapes",
        "odb:ListFlexComponents",
        "odb:ListGiVersions",
        "odb:ListSystemVersions",
        "odb:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:TagResource",
        "odb:UntagResource"
      ],
      "Resource" : [
        "arn:aws:odb:*:*:cloud-vm-cluster/*",
        "arn:aws:odb:*:*:db-node/*"
      ]
    },
    {
      "Sid" : "AllowOutboundIntegrationActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:CreateOutboundIntegration",
```

```
        "odb:UpdateOutboundIntegration"
      ],
      "Resource" : [
        "arn:aws:odb:*:*:cloud-vm-cluster/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonODBExascaleStorageVaultAdmin

Deskripsi: Menyediakan akses administratif untuk mengelola sumber daya vault penyimpanan Exascale di Oracle Database@.AWS

`AmazonODBExascaleStorageVaultAdmin`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonODBExascaleStorageVaultAdmin` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan fungsi pekerjaan
- Waktu pembuatan: 04 September 2026, 21:37 UTC
- Waktu teredit: 04 September 2026, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AmazonODBExascaleStorageVaultAdmin`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowODBActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:GetOciOnboardingStatus",
        "odb:InitializeService",
        "odb:CreateExascaleDbStorageVault",
        "odb:GetExascaleDbStorageVault",
        "odb:UpdateExascaleDbStorageVault",
        "odb:DeleteExascaleDbStorageVault",
        "odb:ListExascaleDbStorageVaults",
        "odb:ListExadbVmClusters",
        "odb:GetDbServer",
        "odb:ListDbServers",
        "odb:ListDbSystemShapes",
        "odb:ListFlexComponents",
        "odb:PutResourcePolicy",
        "odb:GetResourcePolicy",
        "odb:DeleteResourcePolicy",
        "odb:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AllowSLRActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "odb.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:TagResource",
        "odb:UntagResource"
      ],
      "Resource" : [
        "arn:aws:odb:*:*:exascale-db-storage-vault/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonODBExascaleVmClusterAdmin

Deskripsi: Menyediakan akses administratif untuk mengelola sumber daya cluster Exascale VM di Oracle Database@.AWS

`AmazonODBExascaleVmClusterAdmin`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonODBExascaleVmClusterAdmin` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan fungsi pekerjaan
- Waktu pembuatan: 04 September 2026, 21:37 UTC
- Waktu teredit: 04 September 2026, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AmazonODBExascaleVmClusterAdmin`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowODBActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:GetOciOnboardingStatus",
        "odb:InitializeService",
        "odb:GetExascaleDbStorageVault",
        "odb:ListExascaleDbStorageVaults",
```

```
        "odb:CreateExadbVmCluster",
        "odb:GetExadbVmCluster",
        "odb:UpdateExadbVmCluster",
        "odb:DeleteExadbVmCluster",
        "odb:ListExadbVmClusters",
        "odb:AssociateVirtualMachinesToExadbVmCluster",
        "odb:DisassociateVirtualMachinesFromExadbVmCluster",
        "odb:AssociateIamRoleToResource",
        "odb:DisassociateIamRoleFromResource",
        "odb:CreateDbNode",
        "odb:GetDbNode",
        "odb:RebootDbNode",
        "odb:StartDbNode",
        "odb:StopDbNode",
        "odb:DeleteDbNode",
        "odb:ListDbNodes",
        "odb:GetDbServer",
        "odb:ListDbServers",
        "odb:GetOdbNetwork",
        "odb:ListOdbNetworks",
        "odb:ListDbSystemShapes",
        "odb:ListFlexComponents",
        "odb:ListGiVersions",
        "odb:ListGiMinorVersions",
        "odb:ListSystemVersions",
        "odb:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:TagResource",
        "odb:UntagResource"
      ],
```

```
      "Resource" : [
        "arn:aws:odb:*:*:exadb-vm-cluster/*",
        "arn:aws:odb:*:*:db-node/*"
      ]
    },
    {
      "Sid" : "AllowOutboundIntegrationActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:CreateOutboundIntegration",
        "odb:UpdateOutboundIntegration"
      ],
      "Resource" : [
        "arn:aws:odb:*:*:exadb-vm-cluster/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonODBFullAccess

Deskripsi: Menyediakan akses penuh ke sumber daya di Oracle Database@AWS

`AmazonODBFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonODBFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Juli 2026, 22:57 UTC

- Waktu teredit: 04 September 2026, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonODBFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowODBActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:GetOciOnboardingStatus",
        "odb:InitializeService",
        "odb:CreateCloudExadataInfrastructure",
        "odb:GetCloudExadataInfrastructure",
        "odb:UpdateCloudExadataInfrastructure",
        "odb:GetCloudExadataInfrastructureUnallocatedResources",
        "odb:DeleteCloudExadataInfrastructure",
        "odb:ListCloudExadataInfrastructures",
        "odb:CreateCloudVmCluster",
        "odb:GetCloudVmCluster",
        "odb:DeleteCloudVmCluster",
        "odb:ListCloudVmClusters",
        "odb:CreateCloudAutonomousVmCluster",
        "odb:GetCloudAutonomousVmCluster",
        "odb:DeleteCloudAutonomousVmCluster",
        "odb:ListCloudAutonomousVmClusters",
        "odb:CreateExascaleDbStorageVault",
        "odb:GetExascaleDbStorageVault",
        "odb:UpdateExascaleDbStorageVault",
        "odb:DeleteExascaleDbStorageVault",
        "odb:ListExascaleDbStorageVaults",
        "odb:CreateExadbVmCluster",
```

```
        "odb:GetExadbVmCluster",
        "odb:UpdateExadbVmCluster",
        "odb:DeleteExadbVmCluster",
        "odb:ListExadbVmClusters",
        "odb:AssociateVirtualMachinesToExadbVmCluster",
        "odb:DisassociateVirtualMachinesFromExadbVmCluster",
        "odb:ListGiMinorVersions",
        "odb:CreateAutonomousDatabase",
        "odb:GetAutonomousDatabase",
        "odb:UpdateAutonomousDatabase",
        "odb:DeleteAutonomousDatabase",
        "odb:ListAutonomousDatabases",
        "odb:ListAutonomousDatabaseClones",
        "odb:ListAutonomousDatabasePeers",
        "odb:StartAutonomousDatabase",
        "odb:StopAutonomousDatabase",
        "odb:RebootAutonomousDatabase",
        "odb:ShrinkAutonomousDatabase",
        "odb:SwitchoverAutonomousDatabase",
        "odb:FailoverAutonomousDatabase",
        "odb:RestoreAutonomousDatabase",
        "odb:CreateAutonomousDatabaseWallet",
        "odb:GetAutonomousDatabaseWalletDetails",
        "odb:CreateAutonomousDatabaseBackup",
        "odb:GetAutonomousDatabaseBackup",
        "odb:UpdateAutonomousDatabaseBackup",
        "odb:DeleteAutonomousDatabaseBackup",
        "odb:ListAutonomousDatabaseBackups",
        "odb:CreateDbNode",
        "odb:GetDbNode",
        "odb:RebootDbNode",
        "odb:StartDbNode",
        "odb:StopDbNode",
        "odb:DeleteDbNode",
        "odb:ListDbNodes",
        "odb:GetDbServer",
        "odb:ListDbServers",
        "odb:AssociateIamRoleToResource",
        "odb:DisassociateIamRoleFromResource",
        "odb:CreateOdbNetwork",
        "odb:GetOdbNetwork",
        "odb:UpdateOdbNetwork",
        "odb:DeleteOdbNetwork",
        "odb:ListOdbNetworks",
```

```
        "odb:CreateOdbPeeringConnection",
        "odb:GetOdbPeeringConnection",
        "odb:UpdateOdbPeeringConnection",
        "odb:DeleteOdbPeeringConnection",
        "odb:ListOdbPeeringConnections",
        "odb:ListAutonomousVirtualMachines",
        "odb:ListDbSystemShapes",
        "odb:ListFlexComponents",
        "odb:ListGiVersions",
        "odb:ListSystemVersions",
        "odb:ListAutonomousDatabaseVersions",
        "odb:ListAutonomousDatabaseCharacterSets",
        "odb:PutResourcePolicy",
        "odb:GetResourcePolicy",
        "odb:DeleteResourcePolicy",
        "odb:CreateGrantShare",
        "odb:UpdateGrantShare",
        "odb:DeleteGrantShare",
        "odb:CreateOutboundIntegration",
        "odb:UpdateOutboundIntegration",
        "odb:TagResource",
        "odb:UntagResource",
        "odb:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOdbNetworkPeeringActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateOdbNetworkPeering",
        "ec2:ModifyOdbNetworkPeering",
        "ec2:DeleteOdbNetworkPeering"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AllowSLRActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "odb.amazonaws.com",
            "vpc-lattice.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonODBNetworkAdmin

Deskripsi: Menyediakan akses administratif ke sumber daya jaringan untuk Oracle Database@AWS

`AmazonODBNetworkAdmin`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonODBNetworkAdmin` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan fungsi pekerjaan

- Waktu pembuatan: 07 Agustus 2026, 01:12 UTC
- Waktu teredit: 04 September 2026, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AmazonODBNetworkAdmin`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowODBActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:GetOciOnboardingStatus",
        "odb:InitializeService",
        "odb:CreateOdbNetwork",
        "odb:GetOdbNetwork",
        "odb:UpdateOdbNetwork",
        "odb:DeleteOdbNetwork",
        "odb:ListOdbNetworks",
        "odb:CreateOdbPeeringConnection",
        "odb:GetOdbPeeringConnection",
        "odb:UpdateOdbPeeringConnection",
        "odb:DeleteOdbPeeringConnection",
        "odb:ListOdbPeeringConnections",
        "odb:PutResourcePolicy",
        "odb:GetResourcePolicy",
        "odb:DeleteResourcePolicy",
        "odb:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowEC2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOdbNetworkPeeringActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateOdbNetworkPeering",
        "ec2:ModifyOdbNetworkPeering",
        "ec2:DeleteOdbNetworkPeering"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSLRActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "odb.amazonaws.com",
            "vpc-lattice.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:TagResource",
        "odb:UntagResource"
      ],
      "Resource" : [
        "arn:aws:odb:*:*:odb-network/*",
        "arn:aws:odb:*:*:odb-peering-connection/*"
```

```
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonODBReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke sumber daya Oracle Database@AWS

`AmazonODBReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonODBReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Agustus 2026, 01:12 UTC
- Waktu teredit: 04 September 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonODBReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowODBReads",
      "Effect" : "Allow",
      "Action" : [
        "odb:GetOciOnboardingStatus",
        "odb:GetCloudExadataInfrastructure",
        "odb:GetCloudExadataInfrastructureUnallocatedResources",
        "odb:ListCloudExadataInfrastructures",
        "odb:GetCloudVmCluster",
        "odb:ListCloudVmClusters",
        "odb:GetCloudAutonomousVmCluster",
        "odb:ListCloudAutonomousVmClusters",
        "odb:GetExascaleDbStorageVault",
        "odb:ListExascaleDbStorageVaults",
        "odb:GetExadbVmCluster",
        "odb:ListExadbVmClusters",
        "odb:ListGiMinorVersions",
        "odb:GetAutonomousDatabase",
        "odb:ListAutonomousDatabases",
        "odb:ListAutonomousDatabaseClones",
        "odb:ListAutonomousDatabasePeers",
        "odb:GetAutonomousDatabaseBackup",
        "odb:ListAutonomousDatabaseBackups",
        "odb:GetDbNode",
        "odb:ListDbNodes",
        "odb:GetDbServer",
        "odb:ListDbServers",
        "odb:GetOdbNetwork",
        "odb:ListOdbNetworks",
        "odb:GetOdbPeeringConnection",
        "odb:ListOdbPeeringConnections",
        "odb:ListAutonomousVirtualMachines",
        "odb:ListDbSystemShapes",
        "odb:ListFlexComponents",
        "odb:ListGiVersions",
        "odb:ListSystemVersions",
        "odb:ListAutonomousDatabaseVersions",
        "odb:ListAutonomousDatabaseCharacterSets",
```

```
        "odb:GetResourcePolicy",
        "odb:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2Reads",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonODBServiceRolePolicy

Deskripsi: Mengizinkan Oracle Database@AWS mengelola AWS sumber daya atas nama Anda.

`AmazonODBServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 13 November 2024, 18:21 UTC

- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonODBServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/ODB"
          ]
        }
      }
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "NM",
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:GetVpcAttachment",
        "networkmanager:ListAttachments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EB1",
      "Effect" : "Allow",
      "Action" : [
        "events:ActivateEventSource",
        "events:DescribeEventSource"
      ],
      "Resource" : "arn:aws:events:*:*:event-source/aws.partner/odb*"
    },
    {
      "Sid" : "EB2",
      "Effect" : "Allow",
      "Action" : [
        "events:CreateEventBus",
        "events:DescribeEventBus"
      ],
      "Resource" : "arn:aws:events:*:*:event-bus/aws.partner/odb*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonOmicsFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Omics dan lainnya yang diperlukan Layanan AWS. Kebijakan ini memungkinkan pengguna untuk melihat dan menerima undangan berbagi RAM untuk mengakses sumber daya di luar pengguna Akun AWS.

`AmazonOmicsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOmicsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Februari 2023, 00:59 UTC
- Waktu teredit: 24 Februari 2023, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "omics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourceShareInvitations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:CalledViaLast" : "omics.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "omics.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonOmicsReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Omics

`AmazonOmicsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOmicsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2022, 04:17 UTC
- Waktu teredit: 29 November 2022, 04.17 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "omics:Get*",
        "omics:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonOneEnterpriseFullAccess

Deskripsi: Kebijakan ini memberikan izin administratif yang memungkinkan akses ke semua sumber daya dan operasi Amazon One Enterprise.

`AmazonOneEnterpriseFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOneEnterpriseFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2023, 04:58 UTC
- Waktu teredit: 28 November 2023, 04:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FullAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonOneEnterpriseInstallerAccess

Deskripsi: Kebijakan ini memberikan izin baca dan tulis terbatas yang memungkinkan penginstalan dan aktivasi perangkat.

`AmazonOneEnterpriseInstallerAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOneEnterpriseInstallerAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2023, 05:00 UTC
- Waktu teredit: 28 November 2023, 05:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstallerAccessStatementID",
```

```
      "Effect" : "Allow",
      "Action" : [
        "one:CreateDeviceActivationQrCode",
        "one:GetDeviceInstance",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceInstances",
        "one:ListSites"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonOneEnterpriseReadOnlyAccess

Deskripsi: Kebijakan ini memberikan izin baca saja ke semua sumber daya dan operasi Amazon One Enterprise.

`AmazonOneEnterpriseReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOneEnterpriseReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2023, 04:59 UTC
- Waktu teredit: 28 November 2023, 04:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:Get*",
        "one:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonOpenSearchDashboardsServiceRolePolicy

Deskripsi: Menyediakan akses ke OpenSearch Layanan Dasbor Amazon untuk mengakses AWS layanan lain seperti CloudWatch atas nama Anda

`AmazonOpenSearchDashboardsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 22 Desember 2023, 19:38 UTC
- Waktu teredit: 22 Desember 2023, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonOpenSearchDashboardsServiceRoleAllowedActions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AOSD"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonOpenSearchDirectQueryGlueCreateAccess

Deskripsi: Men OpenSearch DirectQuery gizinkan Layanan mengakses API AWS Glue untuk membuat sumber daya atas nama Anda.

`AmazonOpenSearchDirectQueryGlueCreateAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOpenSearchDirectQueryGlueCreateAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Mei 2024, 12:24 UTC
- Waktu teredit: 06 Mei 2024, 12:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchDirectQueryGlueCreateAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "AmazonOpenSearchDirectQueryGlueCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:BatchCreatePartition"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonOpenSearchIngestionFullAccess

Deskripsi: Mengiz OpenSearch inkan Amazon Ingestion mengakses AWS layanan lain atas nama Anda.

`AmazonOpenSearchIngestionFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOpenSearchIngestionFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 April 2023, 18:11 UTC
- Waktu teredit: 26 April 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:CreatePipeline",
        "osis:UpdatePipeline",
        "osis:DeletePipeline",
        "osis:StartPipeline",
        "osis:StopPipeline",
        "osis:ListPipelines",
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:ValidatePipeline",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:TagResource",
        "osis:UntagResource",
        "osis:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/osis.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchIngestionService",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "osis.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonOpenSearchIngestionReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Ing OpenSearch estion Service

`AmazonOpenSearchIngestionReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOpenSearchIngestionReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 April 2023, 18:09 UTC
- Waktu teredit: 26 April 2023, 18:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonOpenSearchIngestionServiceRolePolicy

Deskripsi: Mengiz OpenSearch inkan Amazon Ingestion Service mengakses AWS layanan lain atas nama Anda.

`AmazonOpenSearchIngestionServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 18 November 2022, 16:49 UTC
- Waktu teredit: 28 Agustus 2025, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OSISManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OSISManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/OSIS"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonOpenSearchServerlessServiceRolePolicy

Deskripsi: Izinkan Amazon OpenSearch Serverless mengakses AWS layanan lain seperti CloudWatch API atas nama Anda.

`AmazonOpenSearchServerlessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 24 November 2022, 19:50 UTC
- Waktu teredit: 25 Juli 2024, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAOSSCloudwatchMetrics",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AOSS"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonOpenSearchServiceCognitoAccess

Deskripsi: Menyediakan akses ke layanan konfigurasi Amazon Cognito.

`AmazonOpenSearchServiceCognitoAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOpenSearchServiceCognitoAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 September 2021, 06:31 UTC
- Waktu teredit: 20 Desember 2021, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:UpdateUserPoolClient",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:AdminInitiateAuth",
        "cognito-idp:AdminUserGlobalSignOut",
        "cognito-idp:ListUserPoolClients",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:UpdateIdentityPool",
        "cognito-identity:GetIdentityPoolRoles"
      ],
      "Resource" : [
        "arn:aws:cognito-identity:*:*:identitypool/*",
        "arn:aws:cognito-idp:*:*:userpool/*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "cognito-identity.amazonaws.com",
            "cognito-identity-us-gov.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "cognito-identity:SetIdentityPoolRoles",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonOpenSearchServiceFullAccess

Deskripsi: Menyediakan akses penuh ke OpenSearch layanan konfigurasi Layanan Amazon.

`AmazonOpenSearchServiceFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOpenSearchServiceFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 September 2021, 05:33 UTC
- Waktu teredit: 08 September 2021, 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonOpenSearchServiceReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke OpenSearch layanan konfigurasi Layanan Amazon.

`AmazonOpenSearchServiceReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOpenSearchServiceReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 September 2021, 05:38 UTC
- Waktu teredit: 08 September 2021, 05:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:Describe*",
        "es:List*",
        "es:Get*"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonOpenSearchServiceRolePolicy

Deskripsi: Izinkan Amazon OpenSearch Service mengakses AWS layanan lain seperti EC2 Networking API atas nama Anda.

`AmazonOpenSearchServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 26 Agustus 2021, 09:27 UTC
- Waktu teredit: 27 Maret 2025, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Stmt1480452973134",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973145",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973144",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973165",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973149",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973150",
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnAssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973154",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973164",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973174",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973184",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973194",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973195",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973196",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973197",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/ES",
            "AWS/OpenSearch"
          ]
        }
      }
    },
    {
      "Sid" : "Stmt1480452973198",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973199",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973200",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973201",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973202",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "sso:PutApplicationAccessScope",
      "Resource" : "arn:aws:sso::*:application/*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonPersonalizeFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Personalize melalui Konsol Manajemen AWS dan SDK. Juga menyediakan akses tertentu ke layanan terkait (misalnya, S3, CloudWatch).

`AmazonPersonalizeFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonPersonalizeFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 04 Desember 2018, 22:24 UTC
- Waktu teredit: 30 Mei 2019, 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "personalize:*"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*Personalize*",
        "arn:aws:s3:::*personalize*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "personalize.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonPollyFullAccess

Deskripsi: Memberikan akses penuh ke layanan dan sumber daya Amazon Polly.

`AmazonPollyFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonPollyFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2016, 18:59 UTC
- Waktu teredit: 30 November 2016, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:*"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonPollyReadOnlyAccess

Deskripsi: Memberikan akses baca-saja ke sumber daya Amazon Polly.

`AmazonPollyReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonPollyReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2016, 18:59 UTC
- Waktu teredit: 01 April 2026, 08:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:DescribeVoices",
        "polly:GetLexicon",
        "polly:GetSpeechSynthesisTask",
        "polly:ListLexicons",
        "polly:ListSpeechSynthesisTasks",
        "polly:SynthesizeSpeech",
        "polly:StartSpeechSynthesisStream"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonPrometheusConsoleFullAccess

Deskripsi: Memberikan akses penuh ke sumber daya Prometheus yang AWS dikelola di konsol AWS

`AmazonPrometheusConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonPrometheusConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Desember 2020, 18:11 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagValues",
        "tag:GetTagKeys"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateWorkspace",
        "aps:DescribeWorkspace",
        "aps:UpdateWorkspaceAlias",
        "aps:DeleteWorkspace",
        "aps:ListWorkspaces",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeRuleGroupsNamespace",
        "aps:CreateAlertManagerDefinition",
        "aps:CreateRuleGroupsNamespace",
```

```
        "aps:DeleteAlertManagerDefinition",
        "aps:DeleteRuleGroupsNamespace",
        "aps:ListRuleGroupsNamespaces",
        "aps:PutAlertManagerDefinition",
        "aps:PutRuleGroupsNamespace",
        "aps:TagResource",
        "aps:UntagResource",
        "aps:CreateLoggingConfiguration",
        "aps:UpdateLoggingConfiguration",
        "aps:DeleteLoggingConfiguration",
        "aps:DescribeLoggingConfiguration",
        "aps:UpdateWorkspaceConfiguration",
        "aps:DescribeWorkspaceConfiguration",
        "aps:CreateQueryLoggingConfiguration",
        "aps:UpdateQueryLoggingConfiguration",
        "aps:DeleteQueryLoggingConfiguration",
        "aps:DescribeQueryLoggingConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonPrometheusFullAccess

Deskripsi: Memberikan akses penuh ke sumber daya Prome AWS theus Terkelola

`AmazonPrometheusFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonPrometheusFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Desember 2020, 18:10 UTC
- Waktu teredit: 26 November 2023, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllPrometheusActions",
      "Effect" : "Allow",
      "Action" : [
        "aps:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeCluster",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "aps.amazonaws.com"
```

```
          ]
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scraper.aps.amazonaws.com/
AWSServiceRoleForAmazonPrometheusScraper*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "scraper.aps.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonPrometheusQueryAccess

Deskripsi: Memberikan akses untuk menjalankan kueri terhadap sumber daya Prome AWS theus Terkelola

`AmazonPrometheusQueryAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonPrometheusQueryAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Desember 2020, 01:02 UTC
- Waktu teredit: 19 Desember 2020, 01:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonPrometheusRemoteWriteAccess

Deskripsi: Memberikan akses hanya menulis ke ruang kerja Prome AWS theus Terkelola

`AmazonPrometheusRemoteWriteAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonPrometheusRemoteWriteAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Desember 2020, 01:04 UTC
- Waktu teredit: 19 Desember 2020, 01:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:RemoteWrite"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonPrometheusScraperServiceRolePolicy

Deskripsi: Menyediakan akses ke AWS Sumber Daya yang dikelola atau digunakan oleh Amazon Managed Service untuk Prometheus Collector

`AmazonPrometheusScraperServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 26 November 2023, 14:19 UTC
- Waktu teredit: 17 Juli 2026, 08:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScraperServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeleteSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scraper.aps.amazonaws.com/
AWSServiceRoleForAmazonPrometheusScraper*"
    },
    {
      "Sid" : "NetworkDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ENIManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AMPAgentlessScraper"
          ]
        }
      }
    },
    {
      "Sid" : "TagManagement",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "Null" : {
          "aws:RequestTag/AMPAgentlessScraper" : "false"
        }
      }
    },
    {
      "Sid" : "ENIUpdating",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AMPAgentlessScraper" : "false"
        }
      }
    },
    {
      "Sid" : "EKSAccess",
      "Effect" : "Allow",
      "Action" : "eks:DescribeCluster",
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "DeleteEKSAccessEntry",
      "Effect" : "Allow",
      "Action" : "eks:DeleteAccessEntry",
      "Resource" : "arn:aws:eks:*:*:access-entry/*/role/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        },
        "ArnLike" : {
          "eks:principalArn" : "arn:aws:iam::*:role/aws-service-role/
scraper.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScraper*"
```

```
        }
      }
    },
    {
      "Sid" : "APSWriting",
      "Effect" : "Allow",
      "Action" : "aps:RemoteWrite",
      "Resource" : "arn:aws:aps:*:*:workspace/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchMetricsWriting",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "arn:aws:cloudwatch:*:*:dataset/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonQDeveloperAccess

Deskripsi: Menyediakan akses pengembang untuk mengaktifkan interaksi dengan Amazon Q

`AmazonQDeveloperAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonQDeveloperAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Juli 2024, 08:35 UTC
- Waktu teredit: 20 Mei 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQDeveloperAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAmazonQDeveloperAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
        "q:PassRequest",
        "q:StartTroubleshootingAnalysis",
        "q:StartTroubleshootingResolutionExplanation",
        "q:GetTroubleshootingResults",
        "q:UpdateTroubleshootingCommandResult",
        "q:GetIdentityMetaData",
```

```
        "q:GenerateCodeFromCommands",
        "q:UsePlugin"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCloudControlReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetResource",
        "cloudformation:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "AllowQArtifactsAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:CreateArtifact",
        "q:GetArtifact",
        "q:GetArtifactActionResult",
        "q:PerformArtifactAction"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonQFullAccess

Deskripsi: Menyediakan akses penuh untuk mengaktifkan interaksi dengan Amazon Q

`AmazonQFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonQFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2023, 16:00 UTC
- Waktu teredit: 20 Mei 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQFullAccess`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAmazonQFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
```

```
        "q:PassRequest",
        "q:StartTroubleshootingAnalysis",
        "q:GetTroubleshootingResults",
        "q:StartTroubleshootingResolutionExplanation",
        "q:UpdateTroubleshootingCommandResult",
        "q:GetIdentityMetadata",
        "q:CreateAssignment",
        "q:DeleteAssignment",
        "q:GenerateCodeFromCommands",
        "q:CreatePlugin",
        "q:UpdatePlugin",
        "q:DeletePlugin",
        "q:GetPlugin",
        "q:UsePlugin",
        "q:ListPlugins",
        "q:ListPluginProviders",
        "q:ListTagsForResource",
        "q:UntagResource",
        "q:TagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowQArtifactsAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:CreateArtifact",
        "q:GetArtifact",
        "q:GetArtifactActionResult",
        "q:PerformArtifactAction"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCloudControlReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetResource",
        "cloudformation:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "AllowPassRoleToAmazonQ",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "q.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonQLDBConsoleFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon QLDB melalui. Konsol Manajemen AWS

`AmazonQLDBConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonQLDBConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 September 2019, 18:24 UTC
- Waktu teredit: 04 November 2022, 17.01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:CreateLedger",
        "qldb:UpdateLedger",
        "qldb:UpdateLedgerPermissionsMode",
        "qldb:DeleteLedger",
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ExportJournalToS3",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:CancelJournalKinesisStream",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:StreamJournalToKinesis",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
```

```
        "qldb:TagResource",
        "qldb:UntagResource",
        "qldb:ListTagsForResource",
        "qldb:SendCommand",
        "qldb:ExecuteStatement",
        "qldb:ShowCatalog",
        "qldb:InsertSampleData",
        "qldb:PartiQLCreateTable",
        "qldb:PartiQLCreateIndex",
        "qldb:PartiQLDropTable",
        "qldb:PartiQLDropIndex",
        "qldb:PartiQLUndropTable",
        "qldb:PartiQLDelete",
        "qldb:PartiQLInsert",
        "qldb:PartiQLUpdate",
        "qldb:PartiQLSelect",
        "qldb:PartiQLHistoryFunction",
        "qldb:PartiQLRedact"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dbqms:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:ListStreams",
        "kinesis:DescribeStream"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "qldb.amazonaws.com"
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonQLDBFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon QLDB melalui API layanan.

`AmazonQLDBFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonQLDBFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 September 2019, 18:23 UTC
- Waktu teredit: 04 November 2022, 17.01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:CreateLedger",
        "qldb:UpdateLedger",
        "qldb:UpdateLedgerPermissionsMode",
        "qldb:DeleteLedger",
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ExportJournalToS3",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:CancelJournalKinesisStream",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:StreamJournalToKinesis",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:GetBlock",
        "qldb:TagResource",
        "qldb:UntagResource",
        "qldb:ListTagsForResource",
        "qldb:SendCommand",
        "qldb:PartiQLCreateTable",
        "qldb:PartiQLCreateIndex",
        "qldb:PartiQLDropTable",
        "qldb:PartiQLDropIndex",
        "qldb:PartiQLUndropTable",
        "qldb:PartiQLDelete",
        "qldb:PartiQLInsert",
        "qldb:PartiQLUpdate",
        "qldb:PartiQLSelect",
        "qldb:PartiQLHistoryFunction",
        "qldb:PartiQLRedact"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "qldb.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonQLDBReadOnly

Deskripsi: Menyediakan akses baca saja ke Amazon QLDB.

`AmazonQLDBReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonQLDBReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 September 2019, 18:19 UTC
- Waktu teredit: 02 Juli 2021, 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBReadOnly`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRDSBetaServiceRolePolicy

Deskripsi: Mengizinkan Amazon RDS mengelola AWS sumber daya atas nama Anda.

`AmazonRDSBetaServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 02 Mei 2018, 19:41 UTC
- Waktu teredit: 07 Agustus 2024, 00:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSBetaServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
```

```
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
```

```
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB",
            "AWS/Neptune",
            "AWS/RDS",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds-beta-us-east-1!*"
      ],
      "Condition" : {
```

```
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-beta-us-
east-1"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-beta-us-east-1!*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-beta-us-
east-1"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRDSCustomInstanceProfileRolePolicy

Deskripsi: Mengizinkan Amazon RDS Custom untuk melakukan berbagai tindakan otomatisasi dan tugas manajemen basis data melalui profil instans EC2.

`AmazonRDSCustomInstanceProfileRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRDSCustomInstanceProfileRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Februari 2024, 17:42 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ssmAgentPermission1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "ssmAgentPermission2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetManifest",
        "ssm:PutConfigurePackageResult"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssmAgentPermission3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssmAgentPermission4",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:OpenControlChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssmAgentPermission5",
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "createEc2SnapshotPermission1",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createEc2SnapshotPermission2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createEc2SnapshotPermission3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
```

```
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createTagForEc2SnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateSnapshot",
            "CreateSnapshots"
          ]
        }
      }
    },
    {
      "Sid" : "rdsCustomS3ObjectPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:putObject",
        "s3:getObject",
        "s3:getObjectVersion",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "arn:aws:s3:::do-not-delete-rds-custom-*/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "rdsCustomS3BucketPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucketVersions",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : [
        "arn:aws:s3:::do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "readSecretsFromCpPermission",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createSecretsOnDpPermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : "custom-oracle-rac"
        }
      }
    },
    {
      "Sid" : "publishCwMetricsPermission",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "rdscustom/rds-custom-sqlserver-agent",
            "RDSCustomForOracle/Agent"
          ]
        }
      }
    },
    {
      "Sid" : "putEventsToEventBusPermission",
      "Effect" : "Allow",
      "Action" : "events:PutEvents",
      "Resource" : "arn:aws:events:*:*:event-bus/default"
    },
    {
      "Sid" : "cwlUploadPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutRetentionPolicy",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
```

```
      "Resource" : "arn:aws:logs:*:*:log-group:rds-custom-instance-*"
    },
    {
      "Sid" : "sendMessageToSqsQueuePermission",
      "Effect" : "Allow",
      "Action" : [
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : "custom-sqlserver"
        }
      }
    },
    {
      "Sid" : "managePrivateIpOnEniPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : "custom-oracle-rac"
        }
      }
    },
    {
      "Sid" : "kmsPermissionWithSecret",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
```

```
          "kms:EncryptionContext:SecretARN" : [
            "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
            "arn:aws:secretsmanager:*:*:secret:rds-custom!*"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "kmsPermissionWithS3",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-rds-custom-
*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRDSCustomPreviewServiceRolePolicy

Deskripsi: Kebijakan Peran Layanan Pratinjau Kustom Amazon RDS

`AmazonRDSCustomPreviewServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 08 Oktober 2021, 21:44 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
```

```
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ecc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "ecc1scoping",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping3",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances1",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
```

```
    {
      "Sid" : "eccRunInstances3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "RequireImdsV2",
      "Effect" : "Deny",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringNotEquals" : {
          "ec2:MetadataHttpTokens" : "required"
        },
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances3keyPair1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:DeleteKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
```

```
        "arn:aws:ec2:*:*:key-pair/preview-rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccKeyPair2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:key-pair/preview-rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface1",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "eccNetworkInterface2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "eccNetworkInterface3",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag2",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateKeyPair",
            "RunInstances",
            "CreateNetworkInterface",
            "CreateVolume",
            "CreateSnapshots",
            "CopySnapshot",
            "AllocateAddress"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "eccVolume2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume4snapshot1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
```

```
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshotCopySource",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/snap-*"
    },
    {
      "Sid" : "eccSnapshotCopyDestination",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/${*}"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "iam1",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "iam2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : "arn:aws:iam::*:role/AWSRDSCustom*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cloudtrail1",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetTrailStatus"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "cw1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw2",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
```

```
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw3",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ssm1",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssm2",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ssm4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb1",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
```

```
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb2",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb3",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds-preview.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "eb4",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:EnableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds-preview.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb5",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "secretmanager1",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:preview-rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
```

```
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager2",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RestoreSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:preview-rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager3",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "servicequota1",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "sqs1",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:TagQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "sqs2",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:DeleteQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle"
          ]
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRDSCustomServiceRolePolicy

Deskripsi: Mengizinkan Amazon RDS Custom mengelola AWS sumber daya atas nama Anda.

`AmazonRDSCustomServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 08 Oktober 2021, 21:39 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v19 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "rdscrc",
      "Effect" : "Allow",
      "Action" : [
        "rds:CrossRegionCommunication"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "ecc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping2",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances1",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
```

```
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Sid" : "eccRunInstances3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "eccModifyInstanceAttribute1",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ],
          "ec2:Attribute" : "InstanceType"
        }
      }
    },
    {
      "Sid" : "RequireImdsV2",
      "Effect" : "Deny",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringNotEquals" : {
          "ec2:MetadataHttpTokens" : "required"
        },
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances3keyPair1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:DeleteKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:key-pair/rds-custom!*"
      ],
      "Condition" : {
```

```
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccKeyPair2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:key-pair/rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface1",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface2",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "eccNetworkInterface3",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateKeyPair",
            "RunInstances",
            "CreateNetworkInterface",
            "CreateVolume",
            "CreateSnapshot",
            "CreateSnapshots",
            "CopySnapshot",
            "AllocateAddress",
            "CopyImage"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume2",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume4snapshot1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
```

```
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot4",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshotCopySource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/snap-*"
    },
    {
      "Sid" : "eccSnapshotCopyDestination",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/${*}"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccAmi1",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CopyImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ]
    },
    {
      "Sid" : "iam1",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "iam2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWSRDSCustom*",
        "arn:aws:iam::*:role/service-role/AWSRDSCustom*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cloudtrail1",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetTrailStatus"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
    },
```

```
    {
      "Sid" : "cw1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw2",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw3",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
```

```
    {
      "Sid" : "ssm1",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssm2",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssm4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "ssm5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb1",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb2",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
```

```
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb3",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb4",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:EnableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
```

```
            "custom.rds.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb5",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "secretmanager1",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager2",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RestoreSecret"
```

```
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager3",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "sqs1",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:TagQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-sqlserver",
            "custom-oracle"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "sqs2",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:DeleteQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "servicequota1",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRDSDataFullAccess

Deskripsi: Mengizinkan akses penuh untuk menggunakan API data RDS, API penyimpanan rahasia untuk kredenSIAL database RDS, dan API manajemen kueri konsol DB untuk menjalankan pernyataan SQL pada cluster Aurora Serverless di. Akun AWS

`AmazonRDSDataFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRDSDataFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 November 2018, 21:29 UTC
- Waktu teredit: 20 November 2019, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSDataFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecretsManagerDbCredentialsAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutResourcePolicy",
```

```
        "secretsmanager:PutSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-db-credentials/*"
    },
    {
      "Sid" : "RDSDataServiceAccess",
      "Effect" : "Allow",
      "Action" : [
        "dbqms:CreateFavoriteQuery",
        "dbqms:DescribeFavoriteQueries",
        "dbqms:UpdateFavoriteQuery",
        "dbqms:DeleteFavoriteQueries",
        "dbqms:GetQueryString",
        "dbqms:CreateQueryHistory",
        "dbqms:DescribeQueryHistory",
        "dbqms:UpdateQueryHistory",
        "dbqms:DeleteQueryHistory",
        "rds-data:ExecuteSql",
        "rds-data:ExecuteStatement",
        "rds-data:BatchExecuteStatement",
        "rds-data:BeginTransaction",
        "rds-data:CommitTransaction",
        "rds-data:RollbackTransaction",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets",
        "secretsmanager:GetRandomPassword",
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRDSDirectoryServiceAccess

Deskripsi: Izinkan RDS mengakses Directory Service Managed AD atas nama pelanggan untuk instans SQL Server DB yang bergabung dengan domain.

`AmazonRDSDirectoryServiceAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRDSDirectoryServiceAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Februari 2016, 02:02 UTC
- Waktu teredit: 15 Mei 2019, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
```

```
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRDSEnhancedMonitoringRole

Deskripsi: Menyediakan akses ke Cloudwatch untuk RDS Enhanced Monitoring

`AmazonRDSEnhancedMonitoringRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRDSEnhancedMonitoringRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 November 2015, 19:58 UTC
- Waktu teredit: 11 November 2015, 19:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EnableCreationAndManagementOfRDSCloudwatchLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:RDS*"
      ]
    },
    {
      "Sid" : "EnableCreationAndManagementOfRDSCloudwatchLogStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:RDS*:log-stream:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRDSFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon RDS melalui. Konsol Manajemen AWS

`AmazonRDSFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRDSFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 17 Agustus 2023, 23:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSFullAccess`

Versi kebijakan

Versi kebijakan: v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
```

```
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:GetCoipPoolUsage",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "outposts:GetOutpostInstanceTypes",
        "devops-guru:GetResourceCollection"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "pi:*",
      "Resource" : [
        "arn:aws:pi:*:*:metrics/rds/*",
        "arn:aws:pi:*:*:perf-reports/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "rds.amazonaws.com",
            "rds.application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "devops-guru:SearchInsights",
        "devops-guru:ListAnomaliesForInsight"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "devops-guru:ServiceNames" : [
            "RDS"
          ]
        },
        "Null" : {
          "devops-guru:ServiceNames" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRDSPerformanceInsightsFullAccess

Deskripsi: Menyediakan akses penuh ke RDS Performance Insights melalui Konsol Manajemen AWS

`AmazonRDSPerformanceInsightsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRDSPerformanceInsightsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Agustus 2023, 23:41 UTC
- Waktu teredit: 23 Juli 2026, 00:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSPerformanceInsightsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics"
      ],
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
```

```
    {
      "Sid" : "AmazonRDSPerformanceInsightsAnalisysReportFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:CreatePerformanceAnalysisReport",
        "pi:GetPerformanceAnalysisReport",
        "pi:ListPerformanceAnalysisReportRecommendations",
        "pi:ListPerformanceAnalysisReports",
        "pi:DeletePerformanceAnalysisReport"
      ],
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsTaggingFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:TagResource",
        "pi:UntagResource",
        "pi:ListTagsForResource"
      ],
      "Resource" : "arn:aws:pi:*:*:*/rds/*"
    },
    {
      "Sid" : "AmazonRDSDescribeInstanceAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:ListTagsForResource",
        "rds:DescribeDBShardGroups"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:cluster:*",
        "arn:aws:rds:*:*:shard-group:*"
      ]
    },
    {
      "Sid" : "AmazonCloudWatchReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRDSPerformanceInsightsReadOnly

Deskripsi: Read-Only kebijakan untuk RDS Performance Insights

`AmazonRDSPerformanceInsightsReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRDSPerformanceInsightsReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 April 2022, 00:02 UTC
- Waktu teredit: 22 Juli 2026, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSDescribeDBInstances",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "arn:aws:rds:*:*:db:*"
    },
    {
      "Sid" : "AmazonRDSDescribeDBClusters",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBClusters",
      "Resource" : "arn:aws:rds:*:*:cluster:*"
    },
    {
      "Sid" : "AmazonRDSDescribeDBShardGroups",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBShardGroups",
      "Resource" : "arn:aws:rds:*:*:shard-group:*"
    },
    {
      "Sid" : "AmazonRDSListTagsForResource",
      "Effect" : "Allow",
      "Action" : "rds:ListTagsForResource",
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:shard-group:*",
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsDescribeDimensionKeys",
      "Effect" : "Allow",
      "Action" : "pi:DescribeDimensionKeys",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetDimensionKeyDetails",
      "Effect" : "Allow",
      "Action" : "pi:GetDimensionKeyDetails",
```

```
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetResourceMetadata",
      "Effect" : "Allow",
      "Action" : "pi:GetResourceMetadata",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetResourceMetrics",
      "Effect" : "Allow",
      "Action" : "pi:GetResourceMetrics",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListAvailableResourceDimensions",
      "Effect" : "Allow",
      "Action" : "pi:ListAvailableResourceDimensions",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListAvailableResourceMetrics",
      "Effect" : "Allow",
      "Action" : "pi:ListAvailableResourceMetrics",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetPerformanceAnalysisReport",
      "Effect" : "Allow",
      "Action" : "pi:GetPerformanceAnalysisReport",
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" :
 "AmazonRDSPerformanceInsightsListPerformanceAnalysisReportRecommendations",
      "Effect" : "Allow",
      "Action" : "pi:ListPerformanceAnalysisReportRecommendations",
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListPerformanceAnalysisReports",
      "Effect" : "Allow",
      "Action" : "pi:ListPerformanceAnalysisReports",
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
```

```
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListTagsForResource",
      "Effect" : "Allow",
      "Action" : "pi:ListTagsForResource",
      "Resource" : "arn:aws:pi:*:*:*/rds/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRDSPreviewServiceRolePolicy

Deskripsi: Kebijakan Peran Layanan Pratinjau Amazon RDS

`AmazonRDSPreviewServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 31 Mei 2018, 18:02 UTC
- Waktu teredit: 07 Agustus 2024, 01:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:CrossRegionCommunication"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB-Preview",
            "AWS/Neptune-Preview",
            "AWS/RDS-Preview",
            "AWS/Usage"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds-preview-us-east-2!*"
      ],
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-preview-
us-east-2"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-preview-us-east-2!*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
```

```
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-preview-
us-east-2"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRDSReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon RDS melalui. Konsol Manajemen AWS

`AmazonRDSReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRDSReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 14 April 2023, 12:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:Describe*",
        "rds:ListTagsForResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "devops-guru:GetResourceCollection"
      ],
      "Resource" : "*"
    },
    {
      "Action" : [
        "devops-guru:SearchInsights",
        "devops-guru:ListAnomaliesForInsight"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "devops-guru:ServiceNames" : [
            "RDS"
```

```
          ]
        },
        "Null" : {
          "devops-guru:ServiceNames" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRDSServiceRolePolicy

Deskripsi: Mengizinkan Amazon RDS mengelola AWS sumber daya atas nama Anda.

`AmazonRDSServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 08 Januari 2018, 18:17 UTC
- Waktu teredit: 01 Juli 2024, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CrossRegionCommunication",
      "Effect" : "Allow",
      "Action" : [
        "rds:CrossRegionCommunication"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
```

```
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*",
        "arn:aws:logs:*:*:log-group:/aws/docdb/*",
        "arn:aws:logs:*:*:log-group:/aws/neptune/*"
      ]
    },
    {
      "Sid" : "CloudWatchStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/docdb/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ]
    },
    {
      "Sid" : "Kinesis",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kinesis:CreateStream",
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStream",
        "kinesis:SplitShard",
        "kinesis:MergeShards",
        "kinesis:DeleteStream",
        "kinesis:UpdateShardCount"
      ],
      "Resource" : [
        "arn:aws:kinesis:*:*:stream/aws-rds-das-*"
      ]
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB",
            "AWS/Neptune",
            "AWS/RDS",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Sid" : "SecretsManagerPassword",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
```

```
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds!*"
      ],
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds"
        }
      }
    },
    {
      "Sid" : "SecretsManagerTags",
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds!*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRedshiftAllCommandsFullAccess

Deskripsi: Kebijakan ini mencakup izin untuk menjalankan perintah SQL untuk menyalin, memuat, membongkar, menanyakan, dan menganalisis data di Amazon Redshift. Kebijakan ini juga memberikan izin untuk menjalankan pernyataan tertentu untuk layanan terkait, seperti Amazon S3, Amazon CloudWatch log, Amazon SageMaker, atau AWS Glue.

`AmazonRedshiftAllCommandsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftAllCommandsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 November 2021, 00:48 UTC
- Waktu teredit: 25 November 2021, 02:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateAutoMLJob",
```

```
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:InvokeEndpoint",
        "sagemaker:StopProcessingJob",
        "sagemaker:CreateModel",
        "sagemaker:CreateProcessingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model/*redshift*",
        "arn:aws:sagemaker:*:*:training-job/*redshift*",
        "arn:aws:sagemaker:*:*:automl-job/*redshift*",
        "arn:aws:sagemaker:*:*:compilation-job/*redshift*",
        "arn:aws:sagemaker:*:*:processing-job/*redshift*",
        "arn:aws:sagemaker:*:*:transform-job/*redshift*",
        "arn:aws:sagemaker:*:*:endpoint/*redshift*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Endpoints/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/ProcessingJobs/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/TrainingJobs/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/TransformJobs/*redshift*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "SageMaker",
            "/aws/sagemaker/Endpoints",
            "/aws/sagemaker/ProcessingJobs",
            "/aws/sagemaker/TrainingJobs",
            "/aws/sagemaker/TransformJobs"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:PutBucketCors",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::redshift-downloads",
        "arn:aws:s3:::redshift-downloads/*",
        "arn:aws:s3:::*redshift*",
        "arn:aws:s3:::*redshift*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/Redshift" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan",
        "dynamodb:DescribeTable",
        "dynamodb:Getitem"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/*redshift*",
        "arn:aws:dynamodb:*:*:table/*redshift*/index/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:ListInstances"
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*redshift*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "elasticmapreduce:ListInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "elasticmapreduce:ResourceTag/Redshift" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:*redshift*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*redshift*/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*redshift*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*redshift*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "redshift.amazonaws.com",
            "glue.amazonaws.com",
            "sagemaker.amazonaws.com",
            "athena.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRedshiftDataFullAccess

Deskripsi: Kebijakan ini menyediakan akses penuh ke Amazon Redshift Data API. Kebijakan ini juga memberikan akses cakupan ke layanan lain yang diperlukan.

`AmazonRedshiftDataFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftDataFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 September 2020, 19:23 UTC
- Waktu teredit: 07 April 2023, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "DataAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/RedshiftDataFullAccess" : "*"
        }
      }
    },
    {
      "Sid" : "GetCredentialsForAPIUser",
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentials",
      "Resource" : [
        "arn:aws:redshift:*:*:dbname:*/*",
        "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
      ]
    },
    {
      "Sid" : "GetCredentialsWithFederatedIAMCredentials",
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentialsWithIAM",
```

```
      "Resource" : "arn:aws:redshift:*:*:dbname:*/*"
    },
    {
      "Sid" : "GetCredentialsForServerless",
      "Effect" : "Allow",
      "Action" : "redshift-serverless:GetCredentials",
      "Resource" : "arn:aws:redshift-serverless:*:*:workgroup/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/RedshiftDataFullAccess" : "*"
        }
      }
    },
    {
      "Sid" : "DenyCreateAPIUser",
      "Effect" : "Deny",
      "Action" : "redshift:CreateClusterUser",
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
      ]
    },
    {
      "Sid" : "ServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/redshift-data.amazonaws.com/
AWSServiceRoleForRedshift",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "redshift-data.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRedshiftFederatedAuthorization

Deskripsi: Ini adalah kebijakan kemudahan penggunaan untuk menjalankan kueri dengan Otorisasi Federasi Amazon Redshift

`AmazonRedshiftFederatedAuthorization`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftFederatedAuthorization` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 November 2025, 00:04 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftFederatedAuthorization`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRedshiftFederatedAuthorization",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
```

```
        "glue:GetCatalogs",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetUserDefinedFunctions",
        "glue:CreateDatabase",
        "glue:CreateTable",
        "glue:DeleteDatabase",
        "glue:DeleteTable",
        "glue:UpdateCatalog",
        "glue:UpdateDatabase",
        "glue:UpdateTable",
        "glue:RenameTable",
        "glue:FederateAuthorization"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "glue:FederatedAuthorizationSource" : "Redshift"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftIdentityCenterSetContext",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRedshiftFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Redshift melalui. Konsol Manajemen AWS

`AmazonRedshiftFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 07 Juli 2022, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "redshift:*",
        "redshift-serverless:*",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
```

```
        "ec2:DescribeInternetGateways",
        "sns:CreateTopic",
        "sns:Get*",
        "sns:List*",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DisableAlarmActions",
        "tag:GetResources",
        "tag:UntagResources",
        "tag:GetTagValues",
        "tag:GetTagKeys",
        "tag:TagResources"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "redshift.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataAPIPermissions",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerListPermissions",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerCreateGetPermissions",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/RedshiftDataFullAccess" : "*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRedshiftQueryEditor

Deskripsi: Menyediakan akses penuh ke Editor Kueri Amazon Redshift dan ke kueri yang disimpan melalui. Konsol Manajemen AWS

`AmazonRedshiftQueryEditor`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftQueryEditor` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Oktober 2018, 22:50 UTC
- Waktu teredit: 16 Februari 2021, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials",
        "redshift:ListSchemas",
        "redshift:ListTables",
        "redshift:ListDatabases",
        "redshift:ExecuteQuery",
        "redshift:FetchResults",
        "redshift:CancelQuery",
        "redshift:DescribeClusters",
        "redshift:DescribeQuery",
        "redshift:DescribeTable",
        "redshift:ViewQueriesFromConsole",
```

```
        "redshift:DescribeSavedQueries",
        "redshift:CreateSavedQuery",
        "redshift:DeleteSavedQueries",
        "redshift:ModifySavedQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataAPIPermissions",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "DataAPIIAMSessionPermissionsRestriction",
      "Action" : [
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:ListStatements"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerListPermissions",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "SecretsManagerCreateGetPermissions",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/RedshiftQueryOwner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRedshiftQueryEditorV2FullAccess

Deskripsi: Memberikan akses penuh ke operasi dan sumber daya Amazon Redshift Query Editor V2. Kebijakan ini juga memberikan akses ke layanan lain yang diperlukan. Ini termasuk izin untuk membuat daftar cluster Amazon Redshift, membaca kunci dan alias di AWS KMS dan mengelola rahasia Query Editor V2 di AWS Secrets Manager.

`AmazonRedshiftQueryEditorV2FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftQueryEditorV2FullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 September 2021, 14:06 UTC
- Waktu teredit: 21 Februari 2024, 17:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KeyManagementServicePermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*"
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2Permissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRedshiftQueryEditorV2NoSharing

Deskripsi: Memberikan kemampuan untuk bekerja dengan Amazon Redshift Query Editor V2 tanpa berbagi sumber daya. Prinsipal yang diberikan hanya dapat membaca, memperbarui, dan menghapus sumber dayanya sendiri tetapi tidak dapat membagikannya. Kebijakan ini juga memberikan akses ke layanan lain yang diperlukan. Ini termasuk izin untuk membuat daftar cluster Amazon Redshift dan mengelola rahasia Query Editor V2 dari kepala sekolah di AWS Secrets Manager.

`AmazonRedshiftQueryEditorV2NoSharing`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftQueryEditorV2NoSharing` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 September 2021, 14:18 UTC
- Waktu teredit: 21 Februari 2024, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateFolder",
        "sqlworkbench:PutTab",
        "sqlworkbench:BatchDeleteFolder",
        "sqlworkbench:DeleteTab",
```

```
        "sqlworkbench:GenerateSession",
        "sqlworkbench:GetAccountInfo",
        "sqlworkbench:GetAccountSettings",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:GetUserWorkspaceSettings",
        "sqlworkbench:PutUserWorkspaceSettings",
        "sqlworkbench:ListConnections",
        "sqlworkbench:ListFiles",
        "sqlworkbench:ListTabs",
        "sqlworkbench:UpdateFolder",
        "sqlworkbench:ListRedshiftClusters",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:ListTaggedResources",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:ListNotebooks",
        "sqlworkbench:GetSchemaInference",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateConnection",
        "sqlworkbench:CreateSavedQuery",
        "sqlworkbench:CreateChart",
        "sqlworkbench:CreateNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sqlworkbench:DeleteChart",
        "sqlworkbench:DeleteConnection",
        "sqlworkbench:DeleteSavedQuery",
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:UpdateFileFolder",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook",
        "sqlworkbench:DeleteNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookCell",
        "sqlworkbench:DeleteNotebookCell",
        "sqlworkbench:UpdateNotebookCellContent",
        "sqlworkbench:UpdateNotebookCellLayout",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:CreateNotebookVersion",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:DeleteNotebookVersion",
        "sqlworkbench:RestoreNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
```

```
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-resource-owner"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRedshiftQueryEditorV2ReadSharing

Deskripsi: Memberikan kemampuan untuk bekerja dengan Amazon Redshift Query Editor V2 dengan pembagian sumber daya yang terbatas. Kepala sekolah yang diberikan dapat membaca, menulis, dan berbagi sumber dayanya sendiri. Kepala sekolah yang diberikan dapat membaca sumber daya yang dibagikan dengan timnya tetapi tidak dapat memperbaruinya. Kebijakan ini juga memberikan akses ke layanan lain yang diperlukan. Ini termasuk izin untuk membuat daftar cluster Amazon Redshift dan mengelola rahasia Query Editor V2 dari kepala sekolah di AWS Secrets Manager.

`AmazonRedshiftQueryEditorV2ReadSharing`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftQueryEditorV2ReadSharing` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 September 2021, 14:22 UTC
- Waktu teredit: 21 Februari 2024, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
```

```
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateFolder",
        "sqlworkbench:PutTab",
        "sqlworkbench:BatchDeleteFolder",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:GenerateSession",
        "sqlworkbench:GetAccountInfo",
        "sqlworkbench:GetAccountSettings",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:GetUserWorkspaceSettings",
        "sqlworkbench:PutUserWorkspaceSettings",
        "sqlworkbench:ListConnections",
        "sqlworkbench:ListFiles",
        "sqlworkbench:ListTabs",
        "sqlworkbench:UpdateFolder",
        "sqlworkbench:ListRedshiftClusters",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:ListTaggedResources",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:ListNotebooks",
        "sqlworkbench:GetSchemaInference",
```

```
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateConnection",
        "sqlworkbench:CreateSavedQuery",
        "sqlworkbench:CreateChart",
        "sqlworkbench:CreateNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:DeleteChart",
        "sqlworkbench:DeleteConnection",
        "sqlworkbench:DeleteSavedQuery",
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:UpdateFileFolder",
        "sqlworkbench:ListTagsForResource",
```

```
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook",
        "sqlworkbench:DeleteNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookCell",
        "sqlworkbench:DeleteNotebookCell",
        "sqlworkbench:UpdateNotebookCellContent",
        "sqlworkbench:UpdateNotebookCellLayout",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:CreateNotebookVersion",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:DeleteNotebookVersion",
        "sqlworkbench:RestoreNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-resource-owner"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TeamReadAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2UntagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:UntagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRedshiftQueryEditorV2ReadWriteSharing

Deskripsi: Memberikan kemampuan untuk bekerja dengan Amazon Redshift Query Editor V2 dengan berbagi sumber daya. Kepala sekolah yang diberikan dapat membaca, menulis, dan berbagi sumber dayanya sendiri. Prinsipal yang diberikan dapat membaca dan memperbarui sumber daya yang dibagikan dengan timnya. Kebijakan ini juga memberikan akses ke layanan lain yang diperlukan. Ini termasuk izin untuk membuat daftar cluster Amazon Redshift dan mengelola rahasia Query Editor V2 dari kepala sekolah di AWS Secrets Manager.

`AmazonRedshiftQueryEditorV2ReadWriteSharing`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftQueryEditorV2ReadWriteSharing` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 September 2021, 14:25 UTC
- Waktu teredit: 21 Februari 2024, 17:30 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
```

```
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateFolder",
        "sqlworkbench:PutTab",
        "sqlworkbench:BatchDeleteFolder",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:GenerateSession",
        "sqlworkbench:GetAccountInfo",
        "sqlworkbench:GetAccountSettings",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:GetUserWorkspaceSettings",
        "sqlworkbench:PutUserWorkspaceSettings",
        "sqlworkbench:ListConnections",
        "sqlworkbench:ListFiles",
        "sqlworkbench:ListTabs",
        "sqlworkbench:UpdateFolder",
        "sqlworkbench:ListRedshiftClusters",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:ListTaggedResources",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:ListNotebooks",
        "sqlworkbench:GetSchemaInference",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateConnection",
        "sqlworkbench:CreateSavedQuery",
        "sqlworkbench:CreateChart",
        "sqlworkbench:CreateNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:DeleteChart",
        "sqlworkbench:DeleteConnection",
        "sqlworkbench:DeleteSavedQuery",
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:UpdateFileFolder",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook",
        "sqlworkbench:DeleteNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookCell",
        "sqlworkbench:DeleteNotebookCell",
        "sqlworkbench:UpdateNotebookCellContent",
```

```
        "sqlworkbench:UpdateNotebookCellLayout",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:CreateNotebookVersion",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:DeleteNotebookVersion",
        "sqlworkbench:RestoreNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-resource-owner"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TeamReadWriteAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
```

```
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2UntagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:UntagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
```

```
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRedshiftReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Redshift melalui. Konsol Manajemen AWS

`AmazonRedshiftReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 08 Februari 2024, 00:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRedshiftReadOnlyAccess",
      "Action" : [
        "redshift:Describe*",
        "redshift:ListRecommendations",
        "redshift:ViewQueriesInConsole",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "sns:Get*",
        "sns:List*",
        "cloudwatch:Describe*",
        "cloudwatch:List*",
        "cloudwatch:Get*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```


Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRedshiftServiceLinkedRolePolicy

Deskripsi: Mengizinkan Amazon Redshift untuk memanggil AWS layanan atas nama Anda

`AmazonRedshiftServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 18 September 2017, 19:19 UTC
- Waktu teredit: 19 Februari 2025, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2VpcPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAddresses",
```

```
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteVpcEndpoints",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PublicAccessCreateEip",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "PublicAccessReleaseEip",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "EnableCreationAndManagementOfRedshiftCloudwatchLogGroups",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/redshift/*"
      ]
    },
    {
      "Sid" : "EnableCreationAndManagementOfRedshiftCloudwatchLogStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/redshift/*:log-stream:*"
      ]
    },
    {
      "Sid" : "CreateSecurityGroupWithTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
```

```
        "ec2:RevokeSecurityGroupIngress",
        "ec2:ModifySecurityGroupRules",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "CreateTagsOnResources",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpc",
            "CreateSecurityGroup",
            "CreateSubnet",
            "CreateInternetGateway",
            "CreateRouteTable",
            "AllocateAddress"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "VPCPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Redshift-Serverless",
            "AWS/Redshift"
          ]
        }
      }
    },
    {
      "Sid" : "SecretManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:RotateSecret"
```

```
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:redshift!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "redshift",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerRandomPassword",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IPV6Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "ServiceQuotasToCheckCustomerLimits",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:ec2/L-0263D0A3",
        "arn:aws:servicequotas:*:*:vpc/L-29B6F2EB"
      ]
    },
    {
      "Sid" : "DiscoverRedshiftCatalogs",
      "Effect" : "Allow",
```

```
      "Action" : [
        "glue:GetCatalog",
        "glue:GetCatalogs"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "Bool" : {
          "glue:EnabledForRedshiftAutoDiscovery" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LakeFormationGetMetadataAccessForFederatedCatalogs",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Bool" : {
          "lakeformation:EnabledOnlyForMetaDataAccess" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "glue.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRekognitionCustomLabelsFullAccess

Deskripsi: Kebijakan ini menentukan izin rekognition dan s3 yang diperlukan oleh fitur Label Kustom Amazon Rekognition.

`AmazonRekognitionCustomLabelsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRekognitionCustomLabelsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Januari 2020, 19:18 UTC
- Waktu teredit: 16 Agustus 2022, 20.20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*custom-labels*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rekognition:CreateProject",
        "rekognition:CreateProjectVersion",
        "rekognition:StartProjectVersion",
        "rekognition:StopProjectVersion",
        "rekognition:DescribeProjects",
        "rekognition:DescribeProjectVersions",
        "rekognition:DetectCustomLabels",
        "rekognition:DeleteProject",
        "rekognition:DeleteProjectVersion",
        "rekognition:TagResource",
        "rekognition:UntagResource",
        "rekognition:ListTagsForResource",
        "rekognition:CreateDataset",
        "rekognition:ListDatasetEntries",
        "rekognition:ListDatasetLabels",
        "rekognition:DescribeDataset",
        "rekognition:UpdateDatasetEntries",
        "rekognition:DistributeDatasetEntries",
        "rekognition:DeleteDataset",
        "rekognition:CopyProjectVersion",
        "rekognition:PutProjectPolicy",
        "rekognition:ListProjectPolicies",
        "rekognition:DeleteProjectPolicy"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRekognitionFullAccess

Deskripsi: Akses ke semua Amazon Rekognition API

`AmazonRekognitionFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRekognitionFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2016, 14:40 UTC
- Waktu teredit: 30 November 2016, 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rekognition:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRekognitionReadOnlyAccess

Deskripsi: Akses ke semua Read Recognition API

`AmazonRekognitionReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRekognitionReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2016, 14:58 UTC
- Waktu teredit: 08 November 2023, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRekognitionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "rekognition:CompareFaces",
        "rekognition:DetectFaces",
        "rekognition:DetectLabels",
        "rekognition:ListCollections",
        "rekognition:ListFaces",
        "rekognition:SearchFaces",
        "rekognition:SearchFacesByImage",
        "rekognition:DetectText",
        "rekognition:GetCelebrityInfo",
        "rekognition:RecognizeCelebrities",
        "rekognition:DetectModerationLabels",
        "rekognition:GetLabelDetection",
        "rekognition:GetFaceDetection",
        "rekognition:GetContentModeration",
        "rekognition:GetPersonTracking",
        "rekognition:GetCelebrityRecognition",
        "rekognition:GetFaceSearch",
        "rekognition:GetTextDetection",
        "rekognition:GetSegmentDetection",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListStreamProcessors",
        "rekognition:DescribeProjects",
        "rekognition:DescribeProjectVersions",
        "rekognition:DetectCustomLabels",
        "rekognition:DetectProtectiveEquipment",
        "rekognition:ListTagsForResource",
```

```
        "rekognition:ListDatasetEntries",
        "rekognition:ListDatasetLabels",
        "rekognition:DescribeDataset",
        "rekognition:ListProjectPolicies",
        "rekognition:ListUsers",
        "rekognition:SearchUsers",
        "rekognition:SearchUsersByImage",
        "rekognition:GetMediaAnalysisJob",
        "rekognition:ListMediaAnalysisJobs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRekognitionServiceRole

Deskripsi: Memungkinkan Rekognition untuk memanggil AWS layanan atas nama Anda.

`AmazonRekognitionServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRekognitionServiceRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 29 November 2017, 16:52 UTC
- Waktu teredit: 29 November 2017, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:AmazonRekognition*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords"
      ],
      "Resource" : "arn:aws:kinesis:*:*:stream/AmazonRekognition*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:GetMedia"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRoute53AutoNamingFullAccess

Deskripsi: Menyediakan akses penuh ke semua tindakan Penamaan Otomatis Route 53.

`AmazonRoute53AutoNamingFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53AutoNamingFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Januari 2018, 18:40 UTC
- Waktu teredit: 18 Januari 2018, 18.40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "servicediscovery:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRoute53AutoNamingReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke semua tindakan Penamaan Otomatis Route 53.

`AmazonRoute53AutoNamingReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53AutoNamingReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Januari 2018, 03:02 UTC
- Waktu teredit: 18 Januari 2018, 03:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:Get*",
        "servicediscovery:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRoute53AutoNamingRegistrantAccess

Deskripsi: Menyediakan akses tingkat pendaftar ke tindakan Penamaan Otomatis Route 53.

`AmazonRoute53AutoNamingRegistrantAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53AutoNamingRegistrantAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Maret 2018, 22:33 UTC
- Waktu teredit: 12 Maret 2018, 22:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:ChangeResourceRecordSets",
```

```
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:DeregisterInstance"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRoute53DomainsFullAccess

Deskripsi: Menyediakan akses penuh ke semua tindakan Domain Route53 dan Buat Zona yang Dihosting untuk memungkinkan pembuatan Zona yang Dihosting sebagai bagian dari pendaftaran domain.

`AmazonRoute53DomainsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53DomainsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRoute53DomainsReadOnlyAccess

Deskripsi: Menyediakan akses ke daftar dan tindakan Domain Route53.

`AmazonRoute53DomainsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53DomainsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRoute53FullAccess

Deskripsi: Menyediakan akses penuh ke semua Amazon Route 53 melalui Konsol Manajemen AWS.

`AmazonRoute53FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53FullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53FullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:*",
        "route53domains:*",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistributionTenantByDomain",
        "cloudfront:GetConnectionGroup",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRegions",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticbeanstalk:DescribeEnvironments",
        "es:ListDomainNames",
        "es:DescribeDomains",
        "lightsail:GetContainerServices",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : "arn:aws:apigateway:*::/domainnames"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRoute53GlobalResolverFullAccess

Deskripsi: Menyediakan akses penuh untuk mengambil, membuat daftar, membuat, memperbarui, dan menghapus semua sumber daya Amazon Route 53 Global Resolver.

`AmazonRoute53GlobalResolverFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53GlobalResolverFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Maret 2026, 20:27 UTC
- Waktu teredit: 09 Maret 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53GlobalResolverFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53GlobalResolverFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRegions",
        "route53:GetHostedZone",
        "route53:ListHostedZones",
        "route53globalresolver:AllowVendedLogDeliveryForResource",
        "route53globalresolver:AssociateHostedZone",
        "route53globalresolver:BatchCreateFirewallRule",
        "route53globalresolver:BatchDeleteFirewallRule",
        "route53globalresolver:BatchUpdateFirewallRule",
        "route53globalresolver:CreateAccessSource",
        "route53globalresolver:CreateAccessToken",
        "route53globalresolver:CreateDNSView",
        "route53globalresolver:CreateFirewallDomainList",
        "route53globalresolver:CreateFirewallRule",
        "route53globalresolver:CreateGlobalResolver",
        "route53globalresolver:DeleteAccessSource",
        "route53globalresolver:DeleteAccessToken",
        "route53globalresolver:DeleteDNSView",
        "route53globalresolver:DeleteFirewallDomainList",
        "route53globalresolver:DeleteFirewallRule",
        "route53globalresolver:DeleteGlobalResolver",
        "route53globalresolver:DisableDNSView",
        "route53globalresolver:DisassociateHostedZone",
        "route53globalresolver:EnableDNSView",
        "route53globalresolver:GetAccessSource",
        "route53globalresolver:GetAccessToken",
        "route53globalresolver:GetDNSView",
        "route53globalresolver:GetFirewallDomainList",
        "route53globalresolver:GetFirewallRule",
        "route53globalresolver:GetGlobalResolver",
        "route53globalresolver:GetHostedZoneAssociation",
        "route53globalresolver:GetManagedFirewallDomainList",
        "route53globalresolver:ImportFirewallDomains",
        "route53globalresolver:ListAccessSources",
        "route53globalresolver:ListAccessTokens",
        "route53globalresolver:ListDNSViews",
        "route53globalresolver:ListFirewallDomainLists",
        "route53globalresolver:ListFirewallDomains",
        "route53globalresolver:ListFirewallRules",
```

```
        "route53globalresolver:ListGlobalResolvers",
        "route53globalresolver:ListHostedZoneAssociations",
        "route53globalresolver:ListManagedFirewallDomainLists",
        "route53globalresolver:ListTagsForResource",
        "route53globalresolver:TagResource",
        "route53globalresolver:UntagResource",
        "route53globalresolver:UpdateAccessSource",
        "route53globalresolver:UpdateAccessToken",
        "route53globalresolver:UpdateDNSView",
        "route53globalresolver:UpdateFirewallDomains",
        "route53globalresolver:UpdateFirewallRule",
        "route53globalresolver:UpdateGlobalResolver",
        "route53globalresolver:UpdateHostedZoneAssociation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRoute53GlobalResolverReadOnlyAccess

Deskripsi: Menyediakan akses baca saja untuk mengambil dan mencantumkan semua sumber daya Amazon Route 53 Global Resolver.

`AmazonRoute53GlobalResolverReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53GlobalResolverReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Maret 2026, 20:27 UTC
- Waktu teredit: 09 Maret 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53GlobalResolverReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53GlobalResolverReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53globalresolver:GetAccessSource",
        "route53globalresolver:GetAccessToken",
        "route53globalresolver:GetDNSView",
        "route53globalresolver:GetFirewallDomainList",
        "route53globalresolver:GetFirewallRule",
        "route53globalresolver:GetGlobalResolver",
        "route53globalresolver:GetHostedZoneAssociation",
        "route53globalresolver:GetManagedFirewallDomainList",
        "route53globalresolver:ListAccessSources",
        "route53globalresolver:ListAccessTokens",
        "route53globalresolver:ListDNSViews",
        "route53globalresolver:ListFirewallDomainLists",
        "route53globalresolver:ListFirewallDomains",
        "route53globalresolver:ListFirewallRules",
        "route53globalresolver:ListGlobalResolvers",
        "route53globalresolver:ListHostedZoneAssociations",
```

```
        "route53globalresolver:ListManagedFirewallDomainLists"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRoute53ProfilesFullAccess

Deskripsi: Kebijakan ini memberikan akses penuh ke sumber daya Profil Amazon Route 53.

`AmazonRoute53ProfilesFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53ProfilesFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 April 2024, 18:30 UTC
- Waktu teredit: 27 Agustus 2024, 19:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ProfilesFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ProfilesFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53profiles:AssociateProfile",
        "route53profiles:AssociateResourceToProfile",
        "route53profiles:CreateProfile",
        "route53profiles:DeleteProfile",
        "route53profiles:DisassociateProfile",
        "route53profiles:DisassociateResourceFromProfile",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfilePolicy",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53profiles:PutProfilePolicy",
        "route53profiles:TagResource",
        "route53profiles:UntagResource",
        "route53profiles:UpdateProfileResourceAssociation",
        "route53resolver:GetFirewallConfig",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverRule",
        "ec2:DescribeVpcs",
        "route53:GetHostedZone"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRoute53ProfilesReadOnlyAccess

Deskripsi: Kebijakan ini memberikan akses baca-saja ke sumber daya Profil Amazon Route 53.

`AmazonRoute53ProfilesReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53ProfilesReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 April 2024, 18:29 UTC
- Waktu teredit: 27 Agustus 2024, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ProfilesReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ProfilesReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfilePolicy",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallConfig",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverQueryLogConfig"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRoute53ReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke semua Amazon Route 53 melalui Konsol Manajemen AWS.

`AmazonRoute53ReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 15 November 2016, 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRoute53RecoveryClusterFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Route 53 Recovery Cluster

`AmazonRoute53RecoveryClusterFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53RecoveryClusterFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Agustus 2021, 18:37 UTC
- Waktu teredit: 18 Agustus 2021 18.37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRoute53RecoveryClusterReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Route 53 Recovery Cluster

`AmazonRoute53RecoveryClusterReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53RecoveryClusterReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Agustus 2021, 17:36 UTC
- Waktu teredit: 01 April 2022, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:ListRoutingControls"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRoute53RecoveryControlConfigFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Route 53 Recovery Control Config

`AmazonRoute53RecoveryControlConfigFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53RecoveryControlConfigFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Agustus 2021, 17:48 UTC
- Waktu teredit: 18 Agustus 2021, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRoute53RecoveryControlConfigReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Route 53 Recovery Control Config

`AmazonRoute53RecoveryControlConfigReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53RecoveryControlConfigReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Agustus 2021, 18:01 UTC
- Waktu teredit: 18 Oktober 2023, 17:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeRoutingControlByName",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:GetResourcePolicy",
        "route53-recovery-control-config:ListAssociatedRoute53HealthChecks",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRoute53RecoveryReadinessFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Route 53 Recovery Readiness

`AmazonRoute53RecoveryReadinessFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53RecoveryReadinessFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 18 Agustus 2021, 16:45 UTC
- Waktu teredit: 18 Agustus 2021, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRoute53RecoveryReadinessReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Route 53 Recovery Readiness

`AmazonRoute53RecoveryReadinessReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53RecoveryReadinessReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Agustus 2021, 18:11 UTC
- Waktu teredit: 09 November 2021, 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetReadinessCheckResourceStatus",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListCrossAccountAuthorizations",
        "route53-recovery-readiness:ListReadinessChecks",
```

```
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53-recovery-readiness:ListRules",
        "route53-recovery-readiness:ListTagsForResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetArchitectureRecommendations",
        "route53-recovery-readiness:GetCellReadinessSummary"
      ],
      "Resource" : "arn:aws:route53-recovery-readiness::*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRoute53ResolverFullAccess

Deskripsi: Kebijakan akses penuh untuk Route 53 Resolver

`AmazonRoute53ResolverFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53ResolverFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Mei 2019, 18:10 UTC

- Waktu teredit: 05 Agustus 2024, 20:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ResolverFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:*",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonRoute53ResolverReadOnlyAccess

Deskripsi: Kebijakan baca saja untuk Route 53 Resolver

`AmazonRoute53ResolverReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53ResolverReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Mei 2019, 18:11 UTC
- Waktu teredit: 05 Agustus 2024, 18:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "AmazonRoute53ResolverReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:Get*",
        "route53resolver:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonS3ExpressFullAccess

Deskripsi: Menyediakan akses penuh ke semua bucket direktori S3.

`AmazonS3ExpressFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3ExpressFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 April 2026, 20:42 UTC

- Waktu teredit: 03 April 2026, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ExpressFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3ExpressFullAccess",
      "Effect" : "Allow",
      "Action" : "s3express:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonS3ExpressReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke operasi S3Express untuk bucket direktori S3.

`AmazonS3ExpressReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3ExpressReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 April 2026, 20:42 UTC
- Waktu teredit: 03 April 2026, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ExpressReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3ExpressReadOnlySessionObjectAccess",
      "Effect" : "Allow",
      "Action" : "s3express:CreateSession",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3express:SessionMode" : "ReadOnly"
        }
      }
    },
    {
      "Sid" : "S3ExpressReadOnlyControlPlaneAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
        "s3express:GetAccessPointScope",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:ListAccessPointsForDirectoryBuckets",
        "s3express:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonS3FilesClientFullAccess

Deskripsi: Menyediakan akses klien root ke sistem file S3 Files.

`AmazonS3FilesClientFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3FilesClientFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 April 2026, 12:57 UTC
- Waktu teredit: 07 April 2026, 12:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FilesClientFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3FilesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3files:ClientMount",
        "s3files:ClientWrite",
        "s3files:ClientRootAccess"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonS3FilesClientReadOnlyAccess

Deskripsi: Menyediakan akses klien baca saja ke sistem file S3 Files.

`AmazonS3FilesClientReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3FilesClientReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 April 2026, 12:57 UTC
- Waktu teredit: 07 April 2026, 12:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FilesClientReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3FilesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3files:ClientMount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonS3FilesClientReadWriteAccess

Deskripsi: Menyediakan akses klien baca dan tulis ke sistem file S3 Files.

`AmazonS3FilesClientReadWriteAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3FilesClientReadWriteAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 April 2026, 12:57 UTC
- Waktu teredit: 07 April 2026, 12:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FilesClientReadWriteAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3FilesPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3files:ClientMount",
        "s3files:ClientWrite"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonS3FilesCSIDriverPolicy

Deskripsi: Menyediakan akses manajemen ke sumber daya Amazon S3 Files

`AmazonS3FilesCSIDriverPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3FilesCSIDriverPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 April 2026, 13:12 UTC
- Waktu teredit: 07 April 2026, 13:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3FilesCSIDriverPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowList",
      "Effect" : "Allow",
      "Action" : [
        "s3files:ListAccessPoints",
        "s3files:ListFileSystems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateAccessPoint",
      "Effect" : "Allow",
      "Action" : [
        "s3files:CreateAccessPoint"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "efs.csi.aws.com/cluster"
        }
      }
    },
    {
      "Sid" : "AllowTagNewAccessPoints",
      "Effect" : "Allow",
      "Action" : [
        "s3files:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "s3files:CreateAction" : "CreateAccessPoint"
        },
        "Null" : {
          "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "efs.csi.aws.com/cluster"
        }
      }
    },
    {
      "Sid" : "AllowDeleteAccessPoint",
      "Effect" : "Allow",
      "Action" : "s3files:DeleteAccessPoint",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/efs.csi.aws.com/cluster" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonS3FilesFullAccess

Deskripsi: Menyediakan akses penuh ke semua File S3 melalui Konsol Manajemen AWS.

`AmazonS3FilesFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3FilesFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 April 2026, 12:42 UTC
- Waktu teredit: 07 April 2026, 12:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FilesFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3FilesPermissions",
      "Effect" : "Allow",
      "Action" : "s3files:*",
      "Resource" : "*"
    },
    {
      "Sid" : "EC2NetworkingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "S3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketNotification",
        "s3:PutBucketNotification"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "EventBridgeManage",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "elasticfilesystem.amazonaws.com"
        }
      },
      "Resource" : [
        "arn:aws:events:*:*:rule/DO-NOT-DELETE-S3-Files*"
      ]
    },
    {
      "Sid" : "EventBridgeRead",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListRules",
        "events:ListTargetsByRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/*"
      ]
    },
    {
      "Sid" : "IAMPassRoleForS3Files",
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "elasticfilesystem.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonS3FilesReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke semua File S3 melalui Konsol Manajemen AWS.

`AmazonS3FilesReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3FilesReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 April 2026, 12:57 UTC
- Waktu teredit: 07 April 2026, 12:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FilesReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3FilesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3files:Get*",
        "s3files:List*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonS3FullAccess

Deskripsi: Menyediakan akses penuh ke semua bucket melalui Konsol Manajemen AWS.

`AmazonS3FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3FullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 27 September 2021, 20.16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:*",
        "s3-object-lambda:*"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonS3ObjectLambdaExecutionRolePolicy

Deskripsi: Menye AWS diakan izin fungsi Lambda untuk berinteraksi dengan Amazon S3 Object Lambda. Juga memberikan izin Lambda untuk menulis ke CloudWatch Log.

`AmazonS3ObjectLambdaExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3ObjectLambdaExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 18 Agustus 2021, 10:07 UTC
- Waktu teredit: 18 Agustus 2021, 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonS3OutpostsFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon S3 di Outpost melalui. Konsol Manajemen AWS

`AmazonS3OutpostsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3OutpostsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Oktober 2020, 17:26 UTC
- Waktu teredit: 02 Oktober 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3-outposts:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "datasync:ListTasks",
        "datasync:ListLocations",
        "datasync:DescribeTask",
        "datasync:DescribeLocation*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:ListOutposts",
        "outposts:GetOutpost"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonS3OutpostsReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon S3 di Outpost melalui. Konsol Manajemen AWS

`AmazonS3OutpostsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3OutpostsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Oktober 2020, 18:55 UTC

- Waktu teredit: 02 Oktober 2020 18.55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3-outposts:Get*",
        "s3-outposts:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "datasync:ListTasks",
        "datasync:ListLocations",
        "datasync:DescribeTask",
        "datasync:DescribeLocation*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:ListOutposts",
        "outposts:GetOutpost"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonS3ReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke semua bucket melalui Konsol Manajemen AWS.

`AmazonS3ReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 10 Agustus 2023, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonS3TablesFullAccess

Deskripsi: Menyediakan akses penuh ke semua bucket tabel S3.

`AmazonS3TablesFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3TablesFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2024, 15:21 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3TablesFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToS3TablesReplication",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : [
            "replication.s3tables.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonS3TablesLakeFormationServiceRole

Deskripsi: Kebijakan terkelola ini memberikan izin AWS Lake Formation untuk bertindak pada semua bucket tabel, ruang nama, dan tabel di dalam akun.

`AmazonS3TablesLakeFormationServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3TablesLakeFormationServiceRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Juni 2025, 19:07 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3TablesLakeFormationServiceRole`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForS3ListTableBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3tables:ListTableBuckets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataAccessPermissionsForS3TablesResources",
      "Effect" : "Allow",
      "Action" : [
        "s3tables:CreateTableBucket",
        "s3tables:GetTableBucket",
        "s3tables:CreateNamespace",
        "s3tables:GetNamespace",
        "s3tables:ListNamespaces",
        "s3tables:DeleteNamespace",
        "s3tables:DeleteTableBucket",
        "s3tables:CreateTable",
        "s3tables:DeleteTable",
        "s3tables:GetTable",
        "s3tables:ListTables",
```

```
        "s3tables:RenameTable",
        "s3tables:UpdateTableMetadataLocation",
        "s3tables:GetTableMetadataLocation",
        "s3tables:GetTableData",
        "s3tables:PutTableData",
        "s3tables:PutTableBucketEncryption"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSDataAccessPermissionsForS3TablesResources",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com"
          ],
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3tables:*:*:bucket/*/table/*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSDescribeKeyAccessPermissionsForS3TablesResources",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "kms:ViaService" : [
            "s3tables.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonS3TablesReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke semua bucket tabel S3.

`AmazonS3TablesReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonS3TablesReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2024, 15:21 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3TablesReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:Get*",
        "s3tables:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

Deskripsi: Kebijakan peran layanan yang digunakan oleh layanan Layanan AWS Katalog untuk menyediakan produk dari SageMaker portofolio produk Amazon. Memberikan izin ke serangkaian layanan terkait termasuk CodePipeline, CodeBuild, CodeCommit, L CloudFormation em, dll.

`AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2020, 18:48 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerServiceCatalogAPIGatewayPermission",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:PATCH",
        "apigateway:DELETE"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:launch-source" : "*"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogAPIGatewayPostPermission",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:POST"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:launch-source"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogAPIGatewayPatchPermission",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:PATCH"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/account"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnMutatePermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*",
      "Condition" : {
        "ArnLikeIfExists" : {
          "cloudformation:RoleArn" : [
            "arn:aws:sts::*:assumed-role/AmazonSageMakerServiceCatalog*"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnTagPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnTemplatePermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeBuildPermission",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:UpdateProject"
      ],
```

```
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeCommitPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CreateCommit",
        "codecommit:CreateRepository",
        "codecommit:DeleteRepository",
        "codecommit:GetRepository",
        "codecommit:TagResource"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeCommitListPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodePipelinePermission",
      "Effect" : "Allow",
      "Action" : [
        "codepipeline:CreatePipeline",
        "codepipeline:DeletePipeline",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:StartPipelineExecution",
        "codepipeline:TagResource",
        "codepipeline:UpdatePipeline"
      ],
      "Resource" : [
        "arn:aws:codepipeline:*:*:sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCIAMUserPermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:CreateUserPool",
        "cognito-idp:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:launch-source"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCIAMPermission",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:CreateGroup",
        "cognito-idp:CreateUserPoolDomain",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteGroup",
        "cognito-idp:DeleteUserPool",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:DeleteUserPoolDomain",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:UpdateUserPoolClient"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:launch-source" : "*"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogECRPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:DeleteRepository",
        "ecr:TagResource"
```

```
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogEventBridgePermission",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DeleteRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogFirehosePermission",
      "Effect" : "Allow",
      "Action" : [
        "firehose:CreateDeliveryStream",
        "firehose:DeleteDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "firehose:StartDeliveryStreamEncryption",
        "firehose:StopDeliveryStreamEncryption",
        "firehose:UpdateDestination"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGluePermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker-*",
```

```
        "arn:aws:glue:*:*:table/sagemaker-*",
        "arn:aws:glue:*:*:userDefinedFunction/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueClassiferPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateClassifier",
        "glue:DeleteClassifier",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeleteTrigger",
        "glue:DeleteWorkflow",
        "glue:StopCrawler"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueWorkflowPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateWorkflow"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:workflow/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueJobPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateJob"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:job/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueCrawlerPermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:CreateCrawler",
        "glue:GetCrawler"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:crawler/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueTriggerPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTrigger",
        "glue:GetTrigger"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:trigger/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerServiceCatalog*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogLambdaPermission",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction",
        "lambda:RemovePermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ]
    },
```

```
    {
      "Sid" : "AmazonSageMakerServiceCatalogLambdaTagPermission",
      "Effect" : "Allow",
      "Action" : "lambda:TagResource",
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:*"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogLogGroupPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/apigateway/AccessLogs/*",
        "arn:aws:logs:*:*:log-group::log-stream:*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogS3ReadPermission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "AmazonSageMakerServiceCatalogS3ReadSagemakerResourcePermission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogS3MutatePermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:GetBucketPolicy",
        "s3:PutBucketAcl",
        "s3:PutBucketNotification",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketLogging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketCORS",
        "s3:PutBucketTagging",
        "s3:PutObjectTagging"
      ],
      "Resource" : "arn:aws:s3:::sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogSageMakerPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeWorkteam",
        "sagemaker:CreateCodeRepository",
```

```
        "sagemaker:DescribeCodeRepository",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:DeleteCodeRepository"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogSageMakerTagPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:model-package/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:*"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogSageMakerImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateImage",
        "sagemaker:DeleteImage",
        "sagemaker:DescribeImage",
        "sagemaker:UpdateImage",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:image/*"
      ]
    },
```

```
    {
      "Sid" : "AmazonSageMakerServiceCatalogStepFunctionPermission",
      "Effect" : "Allow",
      "Action" : [
        "states:CreateStateMachine",
        "states:DeleteStateMachine",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeStarPermission",
      "Effect" : "Allow",
      "Action" : "codestar-connections:PassConnection",
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : "codeconnections:PassConnection",
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codestar-connections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codeconnections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerCanvasAIServicesAccess

Deskripsi: Memberikan izin bagi Amazon SageMaker Canvas untuk menggunakan layanan AI untuk mendukung solusi AI siap pakai. Kebijakan ini akan menambahkan lebih banyak izin mutasi untuk layanan karena Amazon SageMaker Canvas menambahkan dukungan.

`AmazonSageMakerCanvasAIServicesAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerCanvasAIServicesAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Maret 2023, 22:36 UTC
- Waktu teredit: 29 November 2023, 14:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServicesAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Textract",
      "Effect" : "Allow",
      "Action" : [
        "textract:AnalyzeDocument",
        "textract:AnalyzeExpense",
        "textract:AnalyzeID",
        "textract:StartDocumentAnalysis",
        "textract:StartExpenseAnalysis",
        "textract:GetDocumentAnalysis",
        "textract:GetExpenseAnalysis"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Rekognition",
      "Effect" : "Allow",
      "Action" : [
        "rekognition:DetectLabels",
        "rekognition:DetectText"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Comprehend",
      "Effect" : "Allow",
      "Action" : [
        "comprehend:BatchDetectDominantLanguage",
        "comprehend:BatchDetectEntities",
        "comprehend:BatchDetectSentiment",
        "comprehend:DetectPiiEntities",
        "comprehend:DetectEntities",
        "comprehend:DetectSentiment",
        "comprehend:DetectDominantLanguage"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "Bedrock",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:ListFoundationModels",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateBedrockResourcesPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateModelCustomizationJob",
        "bedrock:CreateProvisionedModelThroughput",
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:model-customization-job/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker",
            "Canvas"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:RequestTag/Canvas" : "true",
          "aws:ResourceTag/SageMaker" : "true",
          "aws:ResourceTag/Canvas" : "true"
        }
      }
    },
    {
      "Sid" : "GetStopAndDeleteBedrockResourcesPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetCustomModel",
        "bedrock:GetProvisionedModelThroughput",
```

```
        "bedrock:StopModelCustomizationJob",
        "bedrock:DeleteProvisionedModelThroughput"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:model-customization-job/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true",
          "aws:ResourceTag/Canvas" : "true"
        }
      }
    },
    {
      "Sid" : "FoundationModelPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateModelCustomizationJob"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
      ]
    },
    {
      "Sid" : "BedrockFineTuningPassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "bedrock.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerCanvasBedrockAccess

Deskripsi: Kebijakan ini memberikan izin untuk menggunakan Amazon Bedrock di SageMaker Canvas dengan menyediakan akses ke layanan hilir seperti S3.

`AmazonSageMakerCanvasBedrockAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerCanvasBedrockAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Februari 2024, 18:37 UTC
- Waktu teredit: 02 Februari 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3CanvasAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*/Canvas",
        "arn:aws:s3:::sagemaker-*/Canvas/*"
      ]
    },
    {
      "Sid" : "S3BucketAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerCanvasDataPrepFullAccess

Deskripsi: Menyediakan akses penuh ke SageMaker sumber daya dan operasi Amazon untuk persiapan data di Canvas. Kebijakan ini juga menyediakan akses terpilih ke layanan terkait (misalnya, S3, IAM, KMS, RDS, Logs, Redshift, CloudWatch Athena, Glue,, Secrets Manager). EventBridge Kebijakan ini harus dilampirkan ke peran eksekusi SageMaker Domain/User Profil Amazon.

`AmazonSageMakerCanvasDataPrepFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerCanvasDataPrepFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Oktober 2023, 22:56 UTC
- Waktu teredit: 16 Agustus 2024, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerListFeatureGroupOperation",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListFeatureGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerFeatureGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateFeatureGroup",
        "sagemaker:DescribeFeatureGroup"
      ],
```

```
      "Resource" : "arn:aws:sagemaker:*:*:feature-group/*"
    },
    {
      "Sid" : "SageMakerProcessingJobOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateProcessingJob",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:processing-job/*canvas-data-prep*"
    },
    {
      "Sid" : "SageMakerProcessingJobListOperation",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListProcessingJobs",
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPipelineOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribePipeline",
        "sagemaker:CreatePipeline",
        "sagemaker:UpdatePipeline",
        "sagemaker:DeletePipeline",
        "sagemaker:StartPipelineExecution",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:DescribePipelineExecution"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:pipeline/*canvas-data-prep*"
    },
    {
      "Sid" : "KMSListOperations",
      "Effect" : "Allow",
      "Action" : "kms:ListAliases",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSOperations",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
```

```
    {
      "Sid" : "S3Operations",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3GetObjectOperation",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3ListOperations",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "IAMListOperations",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Sid" : "IAMGetOperations",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "IAMPassOperation",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "events.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EventBridgePutOperation",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeOperations",
      "Effect" : "Allow",
      "Action" : [
```

```
        "events:DescribeRule",
        "events:PutTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeTagBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeListTagOperation",
      "Effect" : "Allow",
      "Action" : "events:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Sid" : "GlueOperations",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:SearchTables"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
```

```
    },
    {
      "Sid" : "EMROperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstanceGroups"
      ],
      "Resource" : "arn:aws:elasticmapreduce:*:*:cluster/*"
    },
    {
      "Sid" : "EMRListOperation",
      "Effect" : "Allow",
      "Action" : "elasticmapreduce:ListClusters",
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaListDataCatalogOperation",
      "Effect" : "Allow",
      "Action" : "athena:ListDataCatalogs",
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaQueryExecutionOperations",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*"
    },
    {
      "Sid" : "AthenaDataCatalogOperations",
      "Effect" : "Allow",
      "Action" : [
        "athena:ListDatabases",
        "athena:ListTableMetadata"
      ],
      "Resource" : "arn:aws:athena:*:*:datacatalog/*"
    },
    {
      "Sid" : "RedshiftOperations",
```

```
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftArnBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "arn:aws:redshift:*:*:cluster:*"
    },
    {
      "Sid" : "RedshiftGetCredentialsOperation",
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentials",
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "SecretsManagerARNBasedOperation",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
    },
    {
      "Sid" : "SecretManagerTagBasedOperation",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true",
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RDSOperation",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "LoggingOperation",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/studio:*"
    },
    {
      "Sid" : "EMRServerlessCreateApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:CreateApplication",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListApplications",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "EMRServerlessApplicationOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:UpdateApplication",
        "emr-serverless:GetApplication"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessStartJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:StartJobRun",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListJobRuns",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessJobRunOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:GetJobRun",
        "emr-serverless:CancelJobRun"
```

```
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*/jobruns/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessTagResourceOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:TagResource",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassOperationForEMRServerless",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerCanvasEMRSExecutionAccess-*",
        "arn:aws:iam::*:role/AmazonSageMakerCanvasEMRSExecutionAccess-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "emr-serverless.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerCanvasDirectDeployAccess

Deskripsi: Mengizinkan Amazon SageMaker Canvas membuat, mengelola, dan melihat detail titik akhir untuk titik akhir yang dibuat melalui Canvas. Mengizinkan Amazon SageMaker Canvas mengambil metrik pemanggilan titik akhir dari CloudWatch.

`AmazonSageMakerCanvasDirectDeployAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerCanvasDirectDeployAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Oktober 2023, 18:11 UTC
- Waktu teredit: 06 Oktober 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "SageMakerEndpointPerms",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:InvokeEndpoint",
        "sagemaker:UpdateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:Canvas*",
        "arn:aws:sagemaker:*:*:canvas*"
      ]
    },
    {
      "Sid" : "ReadCWInvocationMetrics",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy

Deskripsi: Kebijakan ini memberikan izin kepada Amazon EMR Serverless untuk layanan seperti S3, yang digunakan oleh Amazon SageMaker Canvas untuk pemrosesan data besar.

`AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juli 2024, 00:35 UTC
- Waktu teredit: 27 Juli 2024, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3Operations",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
```

```
        "arn:aws:s3:::*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3GetObjectOperation",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3ListOperations",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerCanvasForecastAccess

Deskripsi: Kebijakan ini memberikan izin yang biasanya diperlukan untuk menggunakan SageMaker Canvas dengan Amazon Forecast.

`AmazonSageMakerCanvasForecastAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerCanvasForecastAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 24 Agustus 2022, 20:04 UTC
- Waktu teredit: 24 Agustus 2022, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*/Canvas*",
        "arn:aws:s3:::sagemaker-*/canvas*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerCanvasFullAccess

Deskripsi: Menyediakan akses penuh ke sumber daya dan operasi Amazon SageMaker Canvas. Kebijakan ini juga menyediakan akses terpilih ke layanan terkait (misalnya, S3, IAM, VPC, ECR, CloudWatch Logs, Redshift, Secrets Manager, dan Forecast). Kebijakan ini harus dilampirkan ke peran eksekusi SageMaker Domain/User Profil Amazon.

`AmazonSageMakerCanvasFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerCanvasFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 September 2022, 00:44 UTC
- Waktu teredit: 16 Agustus 2024, 04:35 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerUserDetailsAndPackageOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListTags",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPackageGroupOperations",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelPackage"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model-package-group/*"
      ]
    },
    {
      "Sid" : "SageMakerTrainingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateAutoMLJobV2",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:AddTags",
        "sagemaker:DeleteApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*Canvas*",
```

```
        "arn:aws:sagemaker:*:*:*canvas*",
        "arn:aws:sagemaker:*:*:*model-compilation-*"
      ]
    },
    {
      "Sid" : "SageMakerHostingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteModel",
        "sagemaker:InvokeEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:InvokeEndpointAsync"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*Canvas*",
        "arn:aws:sagemaker:*:*:*canvas*"
      ]
    },
    {
      "Sid" : "EC2VPCOperation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECROperations",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMGetOperations",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "IAMPassOperation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LoggingOperation",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
    },
    {
      "Sid" : "S3Operations",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:CreateBucket",
        "s3:GetBucketCors",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
```

```
      ]
    },
    {
      "Sid" : "ReadSageMakerJumpstartArtifacts",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
      ]
    },
    {
      "Sid" : "S3ListOperations",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueOperations",
      "Effect" : "Allow",
      "Action" : "glue:SearchTables",
      "Resource" : [
        "arn:aws:glue:*:*:table/*/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "SecretsManagerARNBasedOperation",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
```

```
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
    {
      "Sid" : "SecretManagerTagBasedOperation",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftOperations",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftGetCredentialsOperation",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
```

```
      ]
    },
    {
      "Sid" : "ForecastOperations",
      "Effect" : "Allow",
      "Action" : [
        "forecast:CreateExplainabilityExport",
        "forecast:CreateExplainability",
        "forecast:CreateForecastEndpoint",
        "forecast:CreateAutoPredictor",
        "forecast:CreateDatasetImportJob",
        "forecast:CreateDatasetGroup",
        "forecast:CreateDataset",
        "forecast:CreateForecast",
        "forecast:CreateForecastExportJob",
        "forecast:CreatePredictorBacktestExportJob",
        "forecast:CreatePredictor",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeExplainability",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeForecastEndpoint",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeDataset",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:GetAccuracyMetrics",
        "forecast:InvokeForecastEndpoint",
        "forecast:GetRecentForecastContext",
        "forecast:DescribePredictor",
        "forecast:TagResource",
        "forecast:DeleteResourceTree"
      ],
      "Resource" : [
        "arn:aws:forecast:*:*:*Canvas*"
      ]
    },
    {
      "Sid" : "RDSOperation",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "IAMPassOperationForForecast",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AutoscalingOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "arn:aws:application-autoscaling:*:*:scalable-target/*",
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "sagemaker",
          "application-autoscaling:scalable-dimension" :
"sagemaker:variant:DesiredInstanceCount"
        }
      }
    },
    {
      "Sid" : "AsyncEndpointOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "sagemaker:DescribeEndpointConfig"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeScalingOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingActivities"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerCloudWatchUpdate",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AutoscalingSageMakerEndpointOperation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AthenaOperation",
      "Action" : [
        "athena:ListTableMetadata",
        "athena:ListDataCatalogs",
        "athena:ListDatabases"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueOperation",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTables"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QuicksightOperation",
      "Action" : [
        "quicksight:ListNamespaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowUseOfKeyInAccount",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Source" : "SageMakerCanvas",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessCreateApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:CreateApplication",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListApplications",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessApplicationOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:UpdateApplication",
        "emr-serverless:StopApplication",
        "emr-serverless:GetApplication",
        "emr-serverless:StartApplication"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "EMRServerlessStartJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:StartJobRun",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListJobRuns",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessJobRunOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:GetJobRun",
        "emr-serverless:CancelJobRun"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*/jobruns/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessTagResourceOperation",
```

```
      "Effect" : "Allow",
      "Action" : "emr-serverless:TagResource",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassOperationForEMRServerless",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerCanvasEMRSExecutionAccess-*",
        "arn:aws:iam::*:role/AmazonSageMakerCanvasEMRSExecutionAccess-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "emr-serverless.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerCanvasSMDataScienceAssistantAccess

Deskripsi: Memberikan izin bagi Amazon SageMaker Canvas untuk menggunakan layanan SageMaker Data Science Assistant. Data Science Assistant saat ini menggunakan Amazon SageMaker dan Amazon Q Developer untuk memproses permintaan pengguna.

`AmazonSageMakerCanvasSMDataScienceAssistantAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerCanvasSMDataScienceAssistantAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Desember 2024, 14:06 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasSMDataScienceAssistantAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerDataScienceAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-data-science-assistant:SendConversation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "AmazonQDeveloperAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:SendMessage",
        "q:StartConversation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerCapacityReservationServiceRolePolicy

Deskripsi: Kebijakan ini memberikan izin kepada Reservasi SageMaker Kapasitas Amazon untuk mempublikasikan CloudWatch metrik ke akun pelanggan untuk visibilitas pemanfaatan.

`AmazonSageMakerCapacityReservationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 08 April 2026, 20:27 UTC
- Waktu teredit: 08 April 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCapacityReservationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudwatchPutMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "aws/sagemaker/CapacityReservations"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerClusterInstanceRolePolicy

Deskripsi: Kebijakan ini memberikan izin yang biasanya diperlukan untuk menggunakan Amazon SageMaker Cluster.

`AmazonSageMakerClusterInstanceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerClusterInstanceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2023, 15:11 UTC
- Waktu teredit: 29 November 2023, 15:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "CloudwatchLogStreamPublishPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*:log-stream:*"
      ]
    },
    {
      "Sid" : "CloudwatchLogGroupCreationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*"
      ]
    },
    {
      "Sid" : "CloudwatchPutMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "/aws/sagemaker/Clusters"
        }
      }
    },
    {
      "Sid" : "DataRetrievalFromS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
```

```
        "arn:aws:s3:::sagemaker-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SSMConnectivityPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerCoreServiceRolePolicy

Deskripsi: Kebijakan terkelola untuk Peran Tertaut Layanan untuk Layanan SageMaker Inti Amazon

`AmazonSageMakerCoreServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 21 Desember 2020, 21:40 UTC
- Waktu teredit: 21 Desember 2020, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:AuthorizedService" : "sagemaker.amazonaws.com"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerEdgeDeviceFleetPolicy

Deskripsi: Menyediakan izin yang diperlukan bagi SageMaker Edge untuk membuat dan mengelola armada perangkat untuk pelanggan menggunakan koneksi cloud default.

`AmazonSageMakerEdgeDeviceFleetPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerEdgeDeviceFleetPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 08 Desember 2020, 16:17 UTC
- Waktu teredit: 08 Desember 2020, 16:17 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeviceS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "SageMakerEdgeApis",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:SendHeartbeat",
        "sagemaker:GetDeviceRegistration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateIoTRoleAlias",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iot:CreateRoleAlias",
        "iot:DescribeRoleAlias",
        "iot:UpdateRoleAlias",
        "iot:ListTagsForResource",
        "iot:TagResource"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:rolealias/SageMakerEdge*"
      ]
    },
    {
      "Sid" : "CreateIoTRoleAliasIamPermissionsGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*SageMaker*",
        "arn:aws:iam::*:role/*Sagemaker*",
        "arn:aws:iam::*:role/*sagemaker*"
      ]
    },
    {
      "Sid" : "CreateIoTRoleAliasIamPermissionsPassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*SageMaker*",
        "arn:aws:iam::*:role/*Sagemaker*",
        "arn:aws:iam::*:role/*sagemaker*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com",
            "credentials.iot.amazonaws.com"
          ]
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerFeatureStoreAccess

Deskripsi: Menyediakan izin yang diperlukan untuk mengaktifkan toko offline untuk grup SageMaker FeatureStore fitur Amazon.

`AmazonSageMakerFeatureStoreAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerFeatureStoreAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2020, 16:24 UTC
- Waktu teredit: 05 Desember 2022 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*/metadata/*",
        "arn:aws:s3:::*Sagemaker*/metadata/*",
        "arn:aws:s3:::*sagemaker*/metadata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTable",
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore",
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon SageMaker melalui Konsol Manajemen AWS dan SDK. Juga menyediakan akses tertentu ke layanan terkait (misalnya, S3, ECR, CloudWatch Log).

`AmazonSageMakerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2017, 13:07 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFullAccess`

Versi kebijakan

Versi kebijakan: v29 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:partner-app/*",
        "arn:aws:sagemaker:*:*:flow-definition/*",
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Sid" : "AllowAddTagsForSpace",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:space/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : "CreateSpace"
        }
      }
    },
    {
      "Sid" : "AllowAddTagsForApp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*"
      ]
    },
```

```
    {
      "Sid" : "AllowUseOfTrainingPlanResources",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateCluster",
        "sagemaker:UpdateCluster",
        "sagemaker:DescribeTrainingPlan"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Sid" : "AllowStudioActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeDomain",
        "sagemaker:ListDomains",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListUserProfiles",
        "sagemaker:DescribeSpace",
        "sagemaker:ListSpaces",
        "sagemaker:DescribeApp",
        "sagemaker:ListApps"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppActionsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*/*/*/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "AllowAppActionsForSharedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Shared"
          ]
        }
      }
    },
    {
      "Sid" : "AllowMutatingActionsOnSharedSpacesWithoutOwner",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
```

```
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private",
            "Shared"
          ]
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowFlowDefinitionActions",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "AllowAWSServiceActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "cognito-idp:AdminAddUserToGroup",
        "cognito-idp:AdminCreateUser",
        "cognito-idp:AdminDeleteUser",
        "cognito-idp:AdminDisableUser",
        "cognito-idp:AdminEnableUser",
        "cognito-idp:AdminRemoveUserFromGroup",
        "cognito-idp:CreateGroup",
        "cognito-idp:CreateUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:CreateUserPoolDomain",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:List*",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:UpdateUserPoolClient",
        "ec2:CreateNetworkInterface",
```

```
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:CreateRepository",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:StartImageScan",
        "elastic-inference:Connect",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "glue:CreateJob",
        "glue:DeleteJob",
        "glue:GetJob*",
        "glue:GetTable*",
        "glue:GetWorkflowRun",
        "glue:ResetJobBookmark",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:UpdateJob",
        "groundtruthlabeling:*",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
```

```
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery",
        "robomaker:CreateSimulationApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:DeleteSimulationApplication",
        "robomaker:CreateSimulationJob",
        "robomaker:DescribeSimulationJob",
        "robomaker:CancelSimulationJob",
        "secretsmanager:ListSecrets",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "sns:ListTopics",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowECRActions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
        "ecr:PutImage"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeCommitActions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
```

```
      "Resource" : [
        "arn:aws:codecommit:*:*:*sagemaker*",
        "arn:aws:codecommit:*:*:*SageMaker*",
        "arn:aws:codecommit:*:*:*Sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeBuildActions",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker*",
        "arn:aws:codebuild:*:*:build/*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowStepFunctionsActions",
      "Action" : [
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:statemachine:*sagemaker*",
        "arn:aws:states:*:*:execution:*sagemaker*:*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowSecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
```

```
    },
    {
      "Sid" : "AllowReadOnlySecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowServiceCatalogProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ProvisionProduct"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
```

```
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*",
        "arn:aws:s3:::*aws-glue*"
      ]
    },
    {
      "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
```

```
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3BucketACL",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowLambdaInvokeFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForRobomaker",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSNSActions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForSageMakerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*AmazonSageMaker*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "robomaker.amazonaws.com",
            "states.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "AllowPassRoleToSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowAthenaActions",
      "Effect" : "Allow",
      "Action" : [
        "athena:ListDataCatalogs",
        "athena:ListDatabases",
        "athena:ListTableMetadata",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowGlueCreateTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueUpdateTable",
```

```
      "Effect" : "Allow",
      "Action" : [
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore"
      ]
    },
    {
      "Sid" : "AllowGlueDeleteTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueGetTablesAndDatabases",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueGetAndCreateDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
```

```
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore",
        "arn:aws:glue:*:*:database/sagemaker_processing",
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:database/sagemaker_data_wrangler"
      ]
    },
    {
      "Sid" : "AllowRedshiftDataActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowRedshiftGetClusterCredentials",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowListTagsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:user-profile/*"
      ]
    },
    {
```

```
      "Sid" : "AllowCloudformationListStackResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AllowS3ExpressObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:CreateSession"
      ],
      "Resource" : [
        "arn:aws:s3express:*:*:bucket/*SageMaker*",
        "arn:aws:s3express:*:*:bucket/*Sagemaker*",
        "arn:aws:s3express:*:*:bucket/*sagemaker*",
        "arn:aws:s3express:*:*:bucket/*aws-glue*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowS3ExpressCreateBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3express:*:*:bucket/*SageMaker*",
        "arn:aws:s3express:*:*:bucket/*Sagemaker*",
        "arn:aws:s3express:*:*:bucket/*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowS3ExpressListBucketActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3express:ListAllMyDirectoryBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerGeospatialExecutionRole

Deskripsi: Kebijakan ini menyediakan akses ke layanan yang umumnya diperlukan untuk menggunakan SageMaker geospasial.

`AmazonSageMakerGeospatialExecutionRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerGeospatialExecutionRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 30 November 2022, 10:08 UTC
- Waktu teredit: 10 Mei 2023, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:GetEarthObservationJob",
      "Resource" : "arn:aws:sagemaker-geospatial:*:*:earth-observation-job/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:GetRasterDataCollection",
      "Resource" : "arn:aws:sagemaker-geospatial:*:*:raster-data-collection/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerGeospatialFullAccess

Deskripsi: Kebijakan ini memberikan izin yang memungkinkan akses penuh ke Amazon SageMaker Geospatial melalui Konsol Manajemen AWS dan SDK.

`AmazonSageMakerGeospatialFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerGeospatialFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 30 November 2022, 10:06 UTC
- Waktu teredit: 30 November 2022, 10:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker-geospatial.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerGroundTruthExecution

Deskripsi: Menyediakan akses ke AWS layanan yang diperlukan untuk menjalankan pekerjaan SageMaker GroundTruth Pelabelan

`AmazonSageMakerGroundTruthExecution`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerGroundTruthExecution` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Juli 2020, 19:30 UTC
- Waktu teredit: 29 April 2022, 20.49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CustomLabelingJobs",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*GtRecipe*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*",
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*GroundTruth*",
        "arn:aws:s3:::*Groundtruth*",
        "arn:aws:s3:::*groundtruth*",
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StreamingQueue",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : "arn:aws:sqs:*:*:*GroundTruth*"
    },
    {
      "Sid" : "StreamingTopicSubscribe",
      "Effect" : "Allow",
      "Action" : "sns:Subscribe",
      "Resource" : [
        "arn:aws:sns:*:*:*GroundTruth*",
        "arn:aws:sns:*:*:*Groundtruth*",
        "arn:aws:sns:*:*:*groundTruth*",
        "arn:aws:sns:*:*:*groundtruth*",
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sageMaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sns:Protocol" : "sqs"
        },
        "StringLike" : {
          "sns:Endpoint" : "arn:aws:sqs:*:*:*GroundTruth*"
        }
      }
    },
    {
      "Sid" : "StreamingTopic",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*GroundTruth*",
        "arn:aws:sns:*:*:*Groundtruth*",
        "arn:aws:sns:*:*:*groundTruth*",
        "arn:aws:sns:*:*:*groundtruth*",
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sageMaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
    {
      "Sid" : "StreamingTopicUnsubscribe",
      "Effect" : "Allow",
      "Action" : [
        "sns:Unsubscribe"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "WorkforceVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ec2:VpceServiceName" : [
            "*sagemaker-task-resources*",
            "aws.sagemaker*labeling*"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerHyperPodGatedModelAccess

Deskripsi: Kebijakan Terkelola Amazon ini memberikan izin yang diperlukan SageMaker HyperPod untuk mengakses model terjaga keamanannya di SageMaker Jumpstart. Hal ini memungkinkan pembuatan URL yang telah ditandatangani sebelumnya untuk konten hub di SageMaker Public Hub.

`AmazonSageMakerHyperPodGatedModelAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerHyperPodGatedModelAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Januari 2026, 01:04 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodGatedModelAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreatePresignedUrlAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateHubContentPresignedUrls"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:hub/SageMakerPublicHub",
        "arn:aws:sagemaker:*:*:hub-content/SageMakerPublicHub/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerHyperPodInferenceAccess

Deskripsi: Kebijakan ini memberikan hak administratif yang diperlukan untuk menyiapkan operator SageMaker HyperPod inferensi. Ini memungkinkan operator inferensi untuk mengakses sumber daya AWS jaringan, Amazon S3, Amazon ECR, Amazon, Manajer AWS Sertifikat CloudWatch, dan SageMaker sumber daya yang diperlukan untuk menyebarkan dan mengelola beban kerja inferensi pada cluster HyperPod

`AmazonSageMakerHyperPodInferenceAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerHyperPodInferenceAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Januari 2026, 20:34 UTC
- Waktu teredit: 20 Juli 2026, 20:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodInferenceAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeleteObjectsPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::hyperpod-tls*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "S3GetObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::hyperpod-tls*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "s3:ExistingObjectTag/CreatedBy" : "HyperPodInference"
        }
      }
    },
    {
      "Sid" : "S3PutObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectTagging"
      ],
      "Resource" : [
        "arn:aws:s3:::hyperpod-tls*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "s3:RequestObjectTag/CreatedBy" : "HyperPodInference"
        }
      }
    },
    {
      "Sid" : "DataCaptureS3",
      "Effect" : "Allow",
      "Action" : "s3:PutObject",
      "Resource" : [
        "arn:aws:s3:::hyperpod-tls*/data-capture/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3ListBucketAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::hyperpod-tls*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataCaptureKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com",
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::hyperpod-tls*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ECRAuthorization",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "ECRRepositoryAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*"
    },
    {
      "Sid" : "EC2DescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2NetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "EKSClusterAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EKSAccessEntryPolicyAssociation",
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DisassociateAccessPolicy"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*",
      "Condition" : {
        "StringEquals" : {
          "eks:policyarn" : "arn:aws:eks::aws:cluster-access-policy/
AmazonSagemakerHyperpodInferenceMonitoringPolicy"
        }
      }
    },
    {
      "Sid" : "EKSAccessEntryListPolicies",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListAssociatedAccessPolicies"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "ELBListAndDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "FSxAccess",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CertificateImportPermission",
      "Effect" : "Allow",
      "Action" : [
        "acm:AddTagsToCertificate",
        "acm:ImportCertificate"
      ],
      "Resource" : "arn:aws:acm:*:*:certificate/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CreatedBy"
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "HyperPodInference",
          "aws:ResourceTag/CreatedBy" : "HyperPodInference",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "CertificateDeletePermission",
      "Effect" : "Allow",
      "Action" : "acm:DeleteCertificate",
      "Resource" : "arn:aws:acm:*:*:certificate/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "HyperPodInference"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerHyperPodInference*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchMetricsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "HyperPodInference"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeModel",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeClusterInference",
        "sagemaker:UpdateClusterInference",
        "sagemaker:DescribeHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpointconfig/*",
        "arn:aws:sagemaker:*:*:cluster/*",
        "arn:aws:sagemaker:*:*:hub-content/*",
        "arn:aws:sagemaker:*:*:hub/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateModel",
```

```
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "HyperPodInference"
        }
      }
    },
    {
      "Sid" : "SageMakerTagging",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : [
            "CreateModel",
            "CreateEndpointConfig",
            "CreateEndpoint"
          ]
        }
      }
    },
    {
      "Sid" : "SageMakerDeleteAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteModel",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint"
      ],
```

```
      "Resource" : [
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "HyperPodInference"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerHyperPodInferenceGatewayAccess

Deskripsi: Kebijakan ini memberikan izin yang diperlukan untuk mengatur dan mengoperasikan gateway SageMaker HyperPod inferensi. Ini memungkinkan gateway untuk mengelola AWS sertifikat Certificate Manager (ACM) untuk penghentian TLS saat menerapkan dan melayani beban kerja inferensi pada cluster. HyperPod

`AmazonSageMakerHyperPodInferenceGatewayAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerHyperPodInferenceGatewayAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 September 2026, 23:27 UTC

- Waktu teredit: 09 September 2026, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodInferenceGatewayAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ImportOwnedCert",
      "Effect" : "Allow",
      "Action" : [
        "acm:ImportCertificate",
        "acm:AddTagsToCertificate"
      ],
      "Resource" : "arn:aws:acm:*:*:certificate/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "HyperPodInference",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "CreatedBy"
          ]
        }
      }
    },
    {
      "Sid" : "ReadOwnedCerts",
      "Effect" : "Allow",
      "Action" : [
```

```
        "acm:DescribeCertificate",
        "acm:ListTagsForCertificate"
      ],
      "Resource" : "arn:aws:acm:*:*:certificate/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "HyperPodInference",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DeleteOwnedImportedCerts",
      "Effect" : "Allow",
      "Action" : [
        "acm:DeleteCertificate"
      ],
      "Resource" : "arn:aws:acm:*:*:certificate/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "HyperPodInference",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "acm:CertificateKeyPairOrigin" : "CUSTOMER_PROVIDED"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerHyperPodObservabilityAdminAccess

Deskripsi: Kebijakan ini memberikan hak administratif yang diperlukan untuk menyiapkan SageMaker HyperPod observabilitas. Ini memungkinkan akses ke Amazon Managed Prometheus, Amazon

Managed Grafana dan EKS Addons. Kebijakan ini juga mencakup akses luas ke Grafana HTTP API melalui ServiceAccountTokens semua ruang kerja Grafana yang Dikelola Amazon di akun Anda.

`AmazonSageMakerHyperPodObservabilityAdminAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerHyperPodObservabilityAdminAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: Juli 10, 2025, 14:37 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodObservabilityAdminAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrometheusCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateWorkspace"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "PrometheusTagsAccess",
      "Effect" : "Allow",
      "Action" : "aps:TagResource",
      "Resource" : [
        "arn:aws:aps:*:*:/workspaces",
        "arn:aws:aps:*:*:rulegroupsnamespace/*/HyperPodObservabilityNamespace"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "PrometheusDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:DescribeWorkspace"
      ],
      "Resource" : "arn:aws:aps:*:*:workspace/*"
    },
    {
      "Sid" : "PrometheusListAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:ListWorkspaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrometheusAlertsRuleGroupAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "aps:CreateAlertManagerDefinition",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeRuleGroupsNamespace",
        "aps:ListRuleGroupsNamespaces"
      ],
      "Resource" : [
        "arn:aws:aps:*:*:workspace/*",
        "arn:aws:aps:*:*:rulegroupsnamespace/*/HyperPodObservabilityNamespace"
      ]
    },
    {
      "Sid" : "PrometheusCreateRuleGroupAccess",
      "Effect" : "Allow",
      "Action" : "aps:CreateRuleGroupsNamespace",
      "Resource" : "arn:aws:aps:*:*:rulegroupsnamespace/*/
HyperPodObservabilityNamespace",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "GrafanaCreateWorkspaceAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:CreateWorkspace"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "GrafanaTagsAccess",
      "Effect" : "Allow",
      "Action" : "grafana:TagResource",
      "Resource" : "arn:aws:grafana:*:*:/workspaces",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
```

```
            "SageMaker"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "GrafanaListAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:ListWorkspaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrafanaServiceAccountAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:CreateWorkspaceApiKey",
        "grafana:CreateWorkspaceServiceAccount",
        "grafana:CreateWorkspaceServiceAccountToken",
        "grafana:ListWorkspaceServiceAccounts",
        "grafana:ListWorkspaceServiceAccountTokens",
        "grafana:DeleteWorkspaceServiceAccountToken"
      ],
      "Resource" : "arn:aws:grafana:*:*:/workspaces/*"
    },
    {
      "Sid" : "IAMGrafanaPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSageMakerHyperPodObservabilityGrafanaAccess-*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "grafana.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "IAMEKSPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSageMakerHyperPodObservabilityAddonAccess-*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "pods.eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMGetRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerHyperPodObservabilityAddonAccess-*"
      ]
    },
    {
      "Sid" : "HyperPodClusterAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListClusters",
        "sagemaker:DescribeCluster"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSAddonAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:DeleteAddon",
        "eks:UpdateAddon",
        "eks:DescribeAddon"
```

```
      ],
      "Resource" : "arn:aws:eks:*:*:addon/*/amazon-sagemaker-hyperpod-observability/*"
    },
    {
      "Sid" : "EKSAddonDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeAddonConfiguration",
        "eks:DescribeAddonVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSAddonPodIdentityAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribePodIdentityAssociation",
        "eks:DeletePodIdentityAssociation",
        "eks:UpdatePodIdentityAssociation"
      ],
      "Resource" : "arn:aws:eks:*:*:podidentityassociation/*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "EKSListDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListAddons",
        "eks:DescribeCluster"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "EKSCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateAddon",
        "eks:CreatePodIdentityAssociation"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "EKSTagsAccess",
      "Effect" : "Allow",
      "Action" : "eks:TagResource",
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*",
        "arn:aws:eks:*:*:addon/*/*/*",
        "arn:aws:eks:*:*:podidentityassociation/*/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "SSOAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:CreateManagedApplicationInstance"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerHyperPodServiceRolePolicy

Deskripsi: Kebijakan ini memberikan izin SageMaker HyperPod kepada Amazon untuk AWS layanan terkait seperti Amazon EKS, Amazon CloudWatch dll.

`AmazonSageMakerHyperPodServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 06 September 2024, 17:04 UTC
- Waktu teredit: 06 September 2024, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerHyperPodServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EKSClusterDescribePermissions",
```

```
      "Effect" : "Allow",
      "Action" : "eks:DescribeCluster",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogStreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*:log-stream:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerHyperPodTrainingOperatorAccess

Deskripsi: Kebijakan ini memberikan izin administratif yang diperlukan untuk mengatur operator SageMaker HyperPod pelatihan. Ini memungkinkan akses ke add-on Amazon SageMaker HyperPod dan EKS. Kebijakan ini mencakup izin untuk menjelaskan SageMaker HyperPod sumber daya di akun Anda.

`AmazonSageMakerHyperPodTrainingOperatorAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerHyperPodTrainingOperatorAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Agustus 2025, 17:04 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodTrainingOperatorAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDescribeClusterNodeOnHyperPodClusters",
```

```
      "Effect" : "Allow",
      "Action" : "sagemaker:DescribeClusterNode",
      "Resource" : "arn:aws:sagemaker:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerInferenceServiceRolePolicy

Deskripsi: Kebijakan terkelola untuk Peran Tertaut Layanan untuk SageMaker Inferensi Amazon.

`AmazonSageMakerInferenceServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 30 Juli 2026, 19:42 UTC
- Waktu teredit: 17 Agustus 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerInferenceServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateENIWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonSageMakerManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "CreateENIInSubnetAndSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
```

```
    {
      "Sid" : "CreateENIPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Permission" : "INSTANCE-ATTACH",
          "aws:ResourceTag/AmazonSageMakerManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "DeleteENITagScoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonSageMakerManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "DeleteENIPermissionTagScoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonSageMakerManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
```

```
      "Sid" : "TagOnCreateSageMakerResourcesForENI",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface",
          "aws:RequestTag/AmazonSageMakerManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DescribeNetworkResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerJobFullAccess

Deskripsi: Memberikan izin untuk peran eksekusi SageMaker pekerjaan Amazon untuk mengakses data di Amazon S3, memanggil agen melalui Amazon Bedrock AgentCore, melacak eksperimen dengan MLFlow, menerbitkan paket model, menulis log ke Amazon, memanggil fungsi AWS Lambda CloudWatch, dan mengelola antarmuka jaringan Amazon VPC.

`AmazonSageMakerJobFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerJobFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Juni 2026, 02:42 UTC
- Waktu teredit: 03 Juni 2026, 02:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerJobFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerHubPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:hub/*",
```

```
        "arn:aws:sagemaker:*:*:hub-content/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerModelPackagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AccessModelPackage",
        "sagemaker:CreateModelPackage",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model-package-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MLflowPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeMlflowApp",
        "sagemaker:CallMlflowAppApi",
        "sagemaker-mlflow:CreateExperiment",
        "sagemaker-mlflow:CreateRun",
        "sagemaker-mlflow:UpdateRun",
        "sagemaker-mlflow:LogBatch",
        "sagemaker-mlflow:GetExperimentByName",
        "sagemaker-mlflow:GetMetricHistory",
        "sagemaker-mlflow:GetRun",
        "sagemaker-mlflow:StartTrace",
        "sagemaker-mlflow:EndTrace",
        "sagemaker-mlflow:SearchTraces",
        "sagemaker-mlflow:ListArtifacts"
```

```
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:mlflow-app/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:InvokeAgentRuntime",
        "bedrock-agentcore:StopRuntimeSession",
        "bedrock-agentcore:GetAgentRuntime"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:runtime/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2NetworkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeDhcpOptions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "EC2NetworkInterfaceTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "EC2NetworkInterfaceDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "LambdaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerJobRuntimeAccess

Deskripsi: Memberikan izin untuk runtime agen untuk memanggil API runtime SageMaker pekerjaan Amazon yang digunakan selama penyesuaian model untuk pembuatan sampel, penyelesaian lintasan, dan pengiriman hadiah.

`AmazonSageMakerJobRuntimeAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerJobRuntimeAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 03 Juni 2026, 02:42 UTC
- Waktu teredit: 07 Agustus 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerJobRuntimeAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerJobRuntimePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:Sample",
        "sagemaker:SampleWithResponseStream",
        "sagemaker:CompleteRollout",
        "sagemaker:UpdateReward"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:job/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BearerTokenPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CallWithBearerToken"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSPermissionsForMTRLRuntime",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerMechanicalTurkAccess

Deskripsi: Menyediakan akses untuk membuat FlowDefinition sumber daya Amazon Augmented AI terhadap tim kerja apa pun.

`AmazonSageMakerMechanicalTurkAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerMechanicalTurkAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 16:19 UTC
- Waktu teredit: 03 Desember 2019, 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerModelCustomizationCoreAccess

Deskripsi: Memberikan izin untuk SageMaker alur kerja penyesuaian model termasuk pelatihan tanpa server, fungsi hadiah khusus untuk pembelajaran penguatan, evaluasi model, dan penerapan ke SageMaker atau titik akhir Bedrock.

`AmazonSageMakerModelCustomizationCoreAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerModelCustomizationCoreAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Mei 2026, 18:57 UTC
- Waktu teredit: 21 Juli 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelCustomizationCoreAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "SageMakerPublicHubPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListHubContents"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
      ]
    },
    {
      "Sid" : "SageMakerHubPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ImportHubContent",
        "sagemaker:ListHubs",
        "sagemaker:ListHubContents",
        "sagemaker:ListHubContentVersions",
        "sagemaker:DescribeHubContent",
        "sagemaker:DeleteHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:hub/*",
        "arn:aws:sagemaker:*:*:hub-content/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "JumpStartS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::jumpstart*"
      ]
    },
    {
      "Sid" : "SageMakerTrainingJob",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:ListTrainingJobs",
        "sagemaker:StopTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerMLFlow",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:UpdateMlflowApp",
        "sagemaker:DescribeMlflowApp",
        "sagemaker:CreatePresignedMlflowAppUrl",
        "sagemaker:CallMlflowAppApi",
        "sagemaker-mlflow:AccessUI",
        "sagemaker-mlflow:GetExperiment",
        "sagemaker-mlflow:GetExperimentByName",
        "sagemaker-mlflow:GetRun",
        "sagemaker-mlflow:GetMetricHistory",
        "sagemaker-mlflow:GetLoggedModel",
        "sagemaker-mlflow:SearchExperiments",
        "sagemaker-mlflow:SearchRuns",
        "sagemaker-mlflow:ListArtifacts",
        "sagemaker-mlflow:CreateExperiment",
        "sagemaker-mlflow:CreateRun",
        "sagemaker-mlflow:LogBatch",
        "sagemaker-mlflow:LogMetric",
        "sagemaker-mlflow:LogParam",
        "sagemaker-mlflow:LogModel",
        "sagemaker-mlflow:LogInputs",
        "sagemaker-mlflow:SetTag",
        "sagemaker-mlflow:UpdateRun"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:mlflow-app/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BYODataSetS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerModelPackage",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:UpdateModelPackage",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:DescribeModel",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model-package-group/*",
```

```
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerLineage",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateAction",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateContext",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:QueryLineage",
        "sagemaker:AddAssociation",
        "sagemaker:UpdateArtifact"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:action/*",
        "arn:aws:sagemaker:*:*:artifact/*",
        "arn:aws:sagemaker:*:*:context/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:experiment-trial-component/*",
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:pipeline/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerPipelines",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePipeline",
        "sagemaker:DescribePipeline",
```

```
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:UpdatePipeline",
        "sagemaker:StartPipelineExecution"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:pipeline/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerInference",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateInferenceComponent",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DeleteInferenceComponent",
        "sagemaker:DeleteEndpoint",
        "sagemaker:InvokeEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:inference-component/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerInferenceAutoscaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets"
```

```
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerInferenceEcrReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListActions",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListEndpoints",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListMlflowApps",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListWorkforces",
        "sagemaker:Search"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "SageMakerTagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model-package-group/*",
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:hub/*",
        "arn:aws:sagemaker:*:*:hub-content/*",
        "arn:aws:sagemaker:*:*:training-job/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:inference-component/*",
        "arn:aws:sagemaker:*:*:action/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerJobAdvancedSettings",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "ec2:DescribeVpcs",
        "servicequotas:ListServiceQuotas"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "CloudWatchLogReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/*",
        "arn:aws:logs:*:*:log-group::log-stream:"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaListFunctions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaPermissionsForRewardFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:InvokeFunction",
        "lambda:GetFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaLayerForAWSSDK",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetLayerVersion"
      ],
      "Resource" : [
        "arn:aws:lambda:*:336392948345:layer:AWSSDK*"
      ]
    },
    {
      "Sid" : "BedrockCustomModelAndEvaluation",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateCustomModel",
        "bedrock:CreateEvaluationJob",
        "bedrock:GetCustomModel",
        "bedrock:GetModelImportJob",
        "bedrock:GetImportedModel",
```

```
        "bedrock:GetEvaluationJob",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:evaluation-job/*",
        "arn:aws:bedrock:*:*:imported-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:model-import-job/*",
        "arn:aws:bedrock:*:*:foundation-model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockModelImportAndList",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateModelImportJob",
        "bedrock:ListProvisionedModelThroughputs",
        "bedrock:ListCustomModelDeployments",
        "bedrock:ListCustomModels",
        "bedrock:ListModelImportJobs"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockFoundationModelOperations",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetFoundationModelAvailability",
        "bedrock:ListFoundationModels"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "PassRoleForSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/*SageMaker*",
        "arn:aws:iam::*:role/service-role/*Sagemaker*",
        "arn:aws:iam::*:role/service-role/*sagemaker*"
      ],
      "Condition" : {
        "ArnLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:sagemaker:*:*:*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "job.sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForAWSLambda",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/SageMakerForLambda*",
        "arn:aws:iam::*:role/service-role/SageMakerForLambda*"
      ],
      "Condition" : {
        "ArnLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:lambda:*:*:function:*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "PassRoleForBedrock",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/SageMakerForBedrock*",
        "arn:aws:iam::*:role/service-role/SageMakerForBedrock*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : "bedrock.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerModelGovernanceUseAccess

Deskripsi: Kebijakan ter AWS kelola ini memberikan izin yang diperlukan untuk menggunakan semua fitur Tata SageMaker Kelola Amazon. Kebijakan ini juga menyediakan akses terpilih ke layanan terkait (misalnya, S3, KMS).

`AmazonSageMakerModelGovernanceUseAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerModelGovernanceUseAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2022, 08:58 UTC
- Waktu teredit: 04 Juni 2024, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSMMonitoringModelCards",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:UpdateMonitoringAlert",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:ListMonitoringAlertHistory",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:CreateModelCard",
        "sagemaker:DescribeModelCard",
        "sagemaker:UpdateModelCard",
        "sagemaker:DeleteModelCard",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelCardVersions",
        "sagemaker:CreateModelCardExportJob",
        "sagemaker:DescribeModelCardExportJob",
```

```
        "sagemaker:ListModelCardExportJobs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSMTrainingModelsSearchTags",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTrainingJobs",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:ListModels",
        "sagemaker:DescribeModel",
        "sagemaker:Search",
        "sagemaker:AddTags",
        "sagemaker:DeleteTags",
        "sagemaker:ListTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKMSActions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3Actions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:CreateBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowS3ListActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerModelRegistryFullAccess

Deskripsi: Ini adalah kebijakan terkelola baru untuk Model Registry di Sagemaker. Kebijakan ini adalah kebijakan mandiri yang dapat dilampirkan ke peran pengguna untuk mengakses fungsionalitas terkait Model Registry di Sagemaker.

`AmazonSageMakerModelRegistryFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerModelRegistryFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 April 2023, 05:20 UTC
- Waktu teredit: 06 Juni 2024, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerModelRegistrySageMakerReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeAction",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:ListAssociations",
        "sagemaker:ListArtifacts",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackages",
        "sagemaker:Search",
        "sagemaker:GetSearchSuggestions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistrySageMakerWritePermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateInferenceRecommendationsJob",
```

```
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteTags",
        "sagemaker:UpdateModelPackage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryS3GetPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryS3ListPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryECRReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:DescribeImages"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryIAMPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryTagReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupGetPermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupListPermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupWritePermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "sagemaker:collection"
        }
      }
    },
```

```
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupDeletePermission",
      "Effect" : "Allow",
      "Action" : "resource-groups:DeleteGroup",
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:collection" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceKMSPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerNotebooksServiceRolePolicy

Deskripsi: Kebijakan terkelola untuk Peran Tertaut Layanan untuk SageMaker Notebook Amazon

`AmazonSageMakerNotebooksServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 18 Oktober 2019, 20:27 UTC
- Waktu teredit: 16 April 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFSxDescribe",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSageMakerDeleteApp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*"
    },
    {
      "Sid" : "AllowEFSAccessPointCreation",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateAccessPoint",
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*",
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSAccessPointDeletion",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DeleteAccessPoint"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:access-point/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSCreation",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateFileSystem",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSMountWithDeletion",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEFSTagging",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:TagResource",
      "Resource" : [
        "arn:aws:elasticfilesystem:*:*:access-point/*",
        "arn:aws:elasticfilesystem:*:*:file-system/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
```

```
    {
      "Sid" : "AllowEC2Tagging",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "AllowEC2Operations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2AuthZ",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
```

```
    },
    {
      "Sid" : "AllowIdcOperations",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateManagedApplicationInstance",
        "sso:DeleteManagedApplicationInstance",
        "sso:GetManagedApplicationInstance"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "AllowSagemakerProfileCreation",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSagemakerSpaceOperationsForCanvasManagedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:DescribeSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:ListTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*/CanvasManagedSpace-*"
    },
    {
      "Sid" : "AllowSagemakerAddTagsForAppManagedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*/CanvasManagedSpace-*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : "CreateSpace"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerPartnerAppsFullAccess

Deskripsi: Memungkinkan pengguna aplikasi SageMaker mitra Amazon untuk mengakses aplikasi, membuat daftar aplikasi yang tersedia, meluncurkan UI web aplikasi, dan terhubung melalui SDK aplikasi.

`AmazonSageMakerPartnerAppsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerPartnerAppsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Januari 2025, 18:37 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPartnerAppsFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerPartnerListAppsPermission",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListPartnerApps",
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AmazonSageMakerPartnerAppsPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePartnerAppPresignedUrl",
        "sagemaker:DescribePartnerApp",
        "sagemaker:CallPartnerAppApi"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:sagemaker:*:*:partner-app/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceR

Deskripsi: Kebijakan peran layanan yang digunakan oleh AWS ApigaGateway dalam produk yang disediakan AWS ServiceCatalog dari portofolio produk Amazon SageMaker . Memberikan izin ke serangkaian layanan terkait termasuk Lambda dan lainnya.

`AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Agustus 2023, 15:06 UTC
- Waktu teredit: 01 Agustus 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:sagemaker-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker:InvokeEndpoint",
      "Resource" : "arn:aws:sagemaker:*:*:endpoint/*",
      "Condition" : {
```

```
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServ

Deskripsi: Kebijakan peran layanan yang digunakan oleh AWS CloudFormation dalam produk AWS ServiceCatalog yang disediakan dari SageMaker portofolio produk Amazon. Memberikan izin ke subset layanan terkait termasuk Lambda, ApiGateway, dan lainnya.

`AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Agustus 2023, 15:06 UTC

- Waktu teredit: 01 Agustus 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsLambdaRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsApiGatewayRole"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "apigateway.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:DeleteFunction",
        "lambda:UpdateFunctionCode",
        "lambda:ListTags",
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:TagResource"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker:project-name",
            "sagemaker:partner"
          ]
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PublishLayerVersion",
        "lambda:GetLayerVersion",
        "lambda:DeleteLayerVersion",
        "lambda:GetFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:layer:sagemaker-*",
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:DELETE",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:POST",
        "apigateway:PUT"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/tags/*"
```

```
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker:project-name",
            "sagemaker:partner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*/lambda-auth-code/layer.zip"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRoleP

Deskripsi: Kebijakan peran layanan yang digunakan oleh AWS Lambda dalam produk AWS ServiceCatalog yang disediakan dari SageMaker portofolio produk Amazon. Memberikan izin ke serangkaian layanan terkait termasuk Manajer Rahasia dan lainnya.

`AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Agustus 2023, 15:05 UTC
- Waktu teredit: 01 Agustus 2023, 15:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:GetSecretValue",
```

```
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:partner" : false
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerPipelinesIntegrations

Deskripsi: Kebijakan Terkelola Amazon ini memberikan izin yang biasanya diperlukan untuk digunakan dengan langkah-langkah Panggilan Balik dan langkah-langkah Lambda di SageMaker Model Building Pipelines. Itu ditambahkan ke AmazonSageMaker-ExecutionRole yang dapat dibuat saat mengatur SageMaker Studio. Itu juga dapat dilampirkan ke peran lain yang akan digunakan untuk menulis atau mengeksekusi pipeline.

`AmazonSageMakerPipelinesIntegrations`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerPipelinesIntegrations` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Juli 2021, 16:35 UTC

- Waktu teredit: 17 Februari 2023, 21:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPipelinesIntegrations`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*sageMaker*",
        "arn:aws:lambda:*:*:function:*SageMaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:*sagemaker*",
        "arn:aws:sqs:*:*:*sageMaker*",
        "arn:aws:sqs:*:*:*SageMaker*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "elasticmapreduce.amazonaws.com",
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/SageMakerPipelineExecutionEMRStepStatusUpdateRule",
        "arn:aws:events:*:*:rule/SageMakerPipelineExecutionEMRClusterStatusUpdateRule"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:CancelSteps",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:RunJobFlow",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:TerminateJobFlows",
        "elasticmapreduce:ListSteps"
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*"
      ]
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerQuickSightVPCPolicy

Deskripsi: Kebijakan ini akan digunakan oleh SageMaker Unified Studios untuk membuat sumber daya terkait VPC untuk QuickSight

`AmazonSageMakerQuickSightVPCPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerQuickSightVPCPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 03 Juni 2025, 17:37 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerQuickSightVPCPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageQuickSightVPCConnection",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateVPCConnection",
        "quicksight:DescribeVPCConnection",
        "quicksight:DeleteVPCConnection",
        "quicksight:ListVPCConnections",
        "quicksight:UpdateVPCConnection"
      ],
      "Resource" : "arn:aws:quicksight:*:*:vpcconnection/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeQuickSightVPCConnectionEC2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "ManageQuickSightEC2NetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerReadOnly

Deskripsi: Menyediakan akses baca saja ke Amazon SageMaker melalui Konsol Manajemen AWS dan SDK.

`AmazonSageMakerReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2017, 13:07 UTC
- Waktu teredit: 01 Desember 2021, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerReadOnly`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sagemaker:BatchGetMetrics",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:BatchGetRecord",
        "sagemaker:GetRecord",
        "sagemaker:Search",
        "sagemaker:QueryLineage",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:GetModelPackageGroupPolicy"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "aws-marketplace:ViewSubscriptions",
        "cloudwatch:DescribeAlarms",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListUsersInGroup",
        "ecr:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePoli

Deskripsi: Kebijakan peran layanan yang digunakan oleh AWS ApigaGateway dalam produk yang disediakan AWS ServiceCatalog dari portofolio produk Amazon SageMaker . Memberikan izin ke serangkaian layanan terkait termasuk CloudWatch Log dan lainnya.

`AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 25 Maret 2022, 04:25 UTC
- Waktu teredit: 25 Maret 2022, 04:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
```

```
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/apigateway/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerServiceCatalogProductsCloudformationServiceRoleP

Deskripsi: Kebijakan peran layanan yang digunakan oleh AWS CloudFormation dalam produk AWS ServiceCatalog yang disediakan dari SageMaker portofolio produk Amazon. Memberikan izin ke subset layanan terkait termasuk SageMaker dan lainnya.

`AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 25 Maret 2022, 04:26 UTC
- Waktu teredit: 25 Maret 2022, 04:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
        "sagemaker:CreateDeviceFleet",
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
```

```
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
        "sagemaker:CreateFlowDefinition",
        "sagemaker:CreateHumanTaskUi",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateImage",
        "sagemaker:CreateImageVersion",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateLineageGroupPolicy",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelBiasJobDefinition",
        "sagemaker:CreateModelExplainabilityJobDefinition",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelQualityJobDefinition",
        "sagemaker:CreateMonitoringSchedule",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateProject",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateTrial",
        "sagemaker:CreateTrialComponent",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteAlgorithm",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteAppImageConfig",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteCodeRepository",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteDataQualityJobDefinition",
        "sagemaker:DeleteDeviceFleet",
        "sagemaker:DeleteDomain",
```

```
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteExperiment",
        "sagemaker:DeleteFeatureGroup",
        "sagemaker:DeleteFlowDefinition",
        "sagemaker:DeleteHumanLoop",
        "sagemaker:DeleteHumanTaskUi",
        "sagemaker:DeleteImage",
        "sagemaker:DeleteImageVersion",
        "sagemaker:DeleteLineageGroupPolicy",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelBiasJobDefinition",
        "sagemaker:DeleteModelExplainabilityJobDefinition",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteModelPackageGroupPolicy",
        "sagemaker:DeleteModelQualityJobDefinition",
        "sagemaker:DeleteMonitoringSchedule",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteProject",
        "sagemaker:DeleteRecord",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteTrial",
        "sagemaker:DeleteTrialComponent",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DeleteWorkforce",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DeregisterDevices",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEdgePackagingJob",
```

```
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanLoop",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeLineageGroup",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSubscribedWorkteam",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:DisableSagemakerServicecatalogPortfolio",
        "sagemaker:DisassociateTrialComponent",
        "sagemaker:EnableSagemakerServicecatalogPortfolio",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:GetRecord",
        "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
```

```
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListCompilationJobs",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDevices",
        "sagemaker:ListDomains",
        "sagemaker:ListEdgePackagingJobs",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceRecommendationsJobs",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListLabelingJobsForWorkteam",
        "sagemaker:ListLineageGroups",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
```

```
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
        "sagemaker:SendHeartbeat",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
```

```
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodeBuildRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ]
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

Deskripsi: Kebijakan peran layanan yang digunakan oleh AWS CodeBuild dalam produk AWS ServiceCatalog yang disediakan dari SageMaker portofolio produk Amazon. Memberikan izin ke subset layanan terkait termasuk CodePipeline, CodeBuild dan lainnya.

`AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Maret 2022, 04:27 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeCommitPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildECRReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeRegistry",
        "ecr:DescribeImageReplicationStatus",
        "ecr:DescribeRepositories",
        "ecr:DescribeImageReplicationStatus",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildECRWritePermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildPassRoletPermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsEventsRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodePipelineRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodeBuildRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "events.amazonaws.com",
            "codepipeline.amazonaws.com",
            "cloudformation.amazonaws.com",
            "codebuild.amazonaws.com",
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildLogPermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*"
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildS3Permission",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
```

```
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildSageMakerPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
        "sagemaker:CreateDeviceFleet",
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
        "sagemaker:CreateFlowDefinition",
        "sagemaker:CreateHumanTaskUi",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateImage",
        "sagemaker:CreateImageVersion",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateLineageGroupPolicy",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelBiasJobDefinition",
        "sagemaker:CreateModelExplainabilityJobDefinition",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelQualityJobDefinition",
```

```
        "sagemaker:CreateMonitoringSchedule",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateProject",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateTrial",
        "sagemaker:CreateTrialComponent",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteAlgorithm",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteAppImageConfig",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteCodeRepository",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteDataQualityJobDefinition",
        "sagemaker:DeleteDeviceFleet",
        "sagemaker:DeleteDomain",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteExperiment",
        "sagemaker:DeleteFeatureGroup",
        "sagemaker:DeleteFlowDefinition",
        "sagemaker:DeleteHumanLoop",
        "sagemaker:DeleteHumanTaskUi",
        "sagemaker:DeleteImage",
        "sagemaker:DeleteImageVersion",
        "sagemaker:DeleteLineageGroupPolicy",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelBiasJobDefinition",
        "sagemaker:DeleteModelExplainabilityJobDefinition",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteModelPackageGroupPolicy",
        "sagemaker:DeleteModelQualityJobDefinition",
        "sagemaker:DeleteMonitoringSchedule",
```

```
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteProject",
        "sagemaker:DeleteRecord",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteTrial",
        "sagemaker:DeleteTrialComponent",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DeleteWorkforce",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DeregisterDevices",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEdgePackagingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanLoop",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeLineageGroup",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
```

```
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSubscribedWorkteam",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:DisableSagemakerServicecatalogPortfolio",
        "sagemaker:DisassociateTrialComponent",
        "sagemaker:EnableSagemakerServicecatalogPortfolio",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:GetRecord",
        "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListCompilationJobs",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDevices",
        "sagemaker:ListDomains",
```

```
        "sagemaker:ListEdgePackagingJobs",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceRecommendationsJobs",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListLabelingJobsForWorkteam",
        "sagemaker:ListLineageGroups",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
```

```
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
        "sagemaker:SendHeartbeat",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
```

```
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:model-package/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeStarConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codestar-connections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
```

```
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

Deskripsi: Kebijakan peran layanan yang digunakan oleh AWS CodePipeline dalam produk AWS ServiceCatalog yang disediakan dari SageMaker portofolio produk Amazon. Memberikan izin ke subset layanan terkait termasuk CodePipeline, CodeBuild dan lainnya.

`AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 Februari 2022, 09:53 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerCodePipelineCFnPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCFnTagPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker:project-name"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineS3Permission",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodePipelinePassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeBuildPermission",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker-*",
        "arn:aws:codebuild:*:*:build/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeCommitPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
```

```
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeStarConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codestar-connections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

Deskripsi: Kebijakan peran layanan yang digunakan oleh AWS CloudWatch Acara dalam AWS ServiceCatalog produk yang disediakan dari SageMaker portofolio produk Amazon. Memberikan izin ke subset layanan terkait termasuk CodePipeline dan lainnya.

`AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 Februari 2022, 09:53 UTC
- Waktu yang telah diedit: 22 Februari 2022, 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "codepipeline:StartPipelineExecution",
      "Resource" : "arn:aws:codepipeline:*:*:sagemaker-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

Deskripsi: Kebijakan peran layanan yang digunakan oleh AWS Firehose dalam produk AWS ServiceCatalog yang disediakan dari SageMaker portofolio produk Amazon. Memberikan izin ke serangkaian layanan terkait termasuk Firehose dan lainnya.

`AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 22 Februari 2022, 09:54 UTC
- Waktu teredit: 22 Februari 2022, 09:54 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

Deskripsi: Kebijakan peran layanan yang digunakan oleh AWS Glue dalam AWS ServiceCatalog produk yang disediakan dari SageMaker portofolio produk Amazon. Memberikan izin ke serangkaian layanan terkait termasuk Glue, S3, dan lainnya.

`AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 Februari 2022, 09:51 UTC
- Waktu teredit: 26 Agustus 2022 19.13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetPartition",
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:DeletePartition",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:GetDatabase",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:SearchTables",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:database/global_temp",
        "arn:aws:glue:*:*:database/sagemaker-*",
        "arn:aws:glue:*:*:table/sagemaker-*",
        "arn:aws:glue:*:*:tableVersion/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/glue/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

Deskripsi: Kebijakan peran layanan yang digunakan oleh AWS Lambda dalam produk AWS ServiceCatalog yang disediakan dari SageMaker portofolio produk Amazon. Memberikan izin ke serangkaian layanan terkait termasuk ECR, S3, dan lainnya.

`AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 04 April 2022, 16:34 UTC
- Waktu teredit: 11 Juni 2024, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerLambdaECRPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeImages",
        "ecr:BatchDeleteImage",
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:DeleteRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaEventBridgePermission",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaS3BucketPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
```

```
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaS3ObjectPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaSageMakerPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
```

```
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
        "sagemaker:CreateDeviceFleet",
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
        "sagemaker:CreateFlowDefinition",
        "sagemaker:CreateHumanTaskUi",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateImage",
        "sagemaker:CreateImageVersion",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateLineageGroupPolicy",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelBiasJobDefinition",
        "sagemaker:CreateModelExplainabilityJobDefinition",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelQualityJobDefinition",
        "sagemaker:CreateMonitoringSchedule",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateProject",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateTrial",
        "sagemaker:CreateTrialComponent",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteAlgorithm",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteAppImageConfig",
```

```
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteCodeRepository",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteDataQualityJobDefinition",
        "sagemaker:DeleteDeviceFleet",
        "sagemaker:DeleteDomain",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteExperiment",
        "sagemaker:DeleteFeatureGroup",
        "sagemaker:DeleteFlowDefinition",
        "sagemaker:DeleteHumanLoop",
        "sagemaker:DeleteHumanTaskUi",
        "sagemaker:DeleteImage",
        "sagemaker:DeleteImageVersion",
        "sagemaker:DeleteLineageGroupPolicy",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelBiasJobDefinition",
        "sagemaker:DeleteModelExplainabilityJobDefinition",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteModelPackageGroupPolicy",
        "sagemaker:DeleteModelQualityJobDefinition",
        "sagemaker:DeleteMonitoringSchedule",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteProject",
        "sagemaker:DeleteRecord",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteTrial",
        "sagemaker:DeleteTrialComponent",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DeleteWorkforce",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DeregisterDevices",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeCodeRepository",
```

```
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEdgePackagingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanLoop",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeLineageGroup",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSubscribedWorkteam",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:DisableSagemakerServicecatalogPortfolio",
        "sagemaker:DisassociateTrialComponent",
```

```
        "sagemaker:EnableSagemakerServicecatalogPortfolio",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:GetRecord",
        "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListCompilationJobs",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDevices",
        "sagemaker:ListDomains",
        "sagemaker:ListEdgePackagingJobs",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceRecommendationsJobs",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListLabelingJobsForWorkteam",
        "sagemaker:ListLineageGroups",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
```

```
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
        "sagemaker:SendHeartbeat",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
```

```
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:action/*",
        "arn:aws:sagemaker:*:*:algorithm/*",
        "arn:aws:sagemaker:*:*:app-image-config/*",
        "arn:aws:sagemaker:*:*:artifact/*",
        "arn:aws:sagemaker:*:*:automl-job/*",
        "arn:aws:sagemaker:*:*:code-repository/*",
        "arn:aws:sagemaker:*:*:compilation-job/*",
        "arn:aws:sagemaker:*:*:context/*",
        "arn:aws:sagemaker:*:*:data-quality-job-definition/*",
        "arn:aws:sagemaker:*:*:device-fleet/*/device/*",
        "arn:aws:sagemaker:*:*:device-fleet/*",
```

```
        "arn:aws:sagemaker:*:*:edge-packaging-job/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:experiment/*",
        "arn:aws:sagemaker:*:*:experiment-trial/*",
        "arn:aws:sagemaker:*:*:experiment-trial-component/*",
        "arn:aws:sagemaker:*:*:feature-group/*",
        "arn:aws:sagemaker:*:*:human-loop/*",
        "arn:aws:sagemaker:*:*:human-task-ui/*",
        "arn:aws:sagemaker:*:*:hyper-parameter-tuning-job/*",
        "arn:aws:sagemaker:*:*:image/*",
        "arn:aws:sagemaker:*:*:image-version/*/*",
        "arn:aws:sagemaker:*:*:inference-recommendations-job/*",
        "arn:aws:sagemaker:*:*:labeling-job/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:model-bias-job-definition/*",
        "arn:aws:sagemaker:*:*:model-explainability-job-definition/*",
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model-package-group/*",
        "arn:aws:sagemaker:*:*:model-quality-job-definition/*",
        "arn:aws:sagemaker:*:*:monitoring-schedule/*",
        "arn:aws:sagemaker:*:*:notebook-instance/*",
        "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:pipeline/*/execution/*",
        "arn:aws:sagemaker:*:*:processing-job/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:training-job/*",
        "arn:aws:sagemaker:*:*:transform-job/*",
        "arn:aws:sagemaker:*:*:workforce/*",
        "arn:aws:sagemaker:*:*:workteam/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ]
    },
```

```
    {
      "Sid" : "AmazonSageMakerLambdaLogPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    },
    {
      "Sid" : "AmazonSageMakerLambdaCodeBuildPermission",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:StartBuild",
        "codebuild:BatchGetBuilds"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/sagemaker-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:project-name" : "*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerSpacesControllerPolicy

Deskripsi: Memberikan izin aktivasi Manajer Sistem, manajemen sesi, dan operasi kunci KMS yang diperlukan untuk Sp SageMaker aces Addon untuk mengaktifkan akses jarak jauh yang aman ke EKS SageMaker Spaces.

`AmazonSageMakerSpacesControllerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerSpacesControllerPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 November 2025, 04:34 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerSpacesControllerPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOperatorToSSMCreateActivationForSpaces",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateActivation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "aws:RequestTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeActivations",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeActivations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeSessions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeSessions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToSSMDeleteActivation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteActivation"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToAddTagsToActivation",
      "Effect" : "Allow",
      "Action" : "ssm:AddTagsToResource",
      "Resource" : [
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:iam::*:role/sagemaker-space-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "aws:RequestTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeManagedNodes",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToSSMDeregisterWorkspaceInstances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeregisterManagedInstance"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "ssm:resourceTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
```

```
      "Sid" : "AllowOperatorToPassSsmManagedNodeRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/sagemaker-space-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToSSMStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "ssm:resourceTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowStartSessionDocuments",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-StartSSHSession",
        "arn:aws:ssm:*:*:document/SageMaker-Space*"
      ]
    },
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
```

```
    },
    {
      "Sid" : "KMSKeyOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:sagemaker:component" : "amazon-sagemaker-spaces",
          "kms:EncryptionContext:sagemaker:eks-cluster-arn" : "${aws:PrincipalTag/eks-
cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeDocument",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/SageMaker-Space*"
      ]
    },
    {
      "Sid" : "AllowOperatorToSSMCreateDocument",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SageMaker-Space*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "aws:RequestTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
```

```
      "Sid" : "AllowOperatorToEnableAdvancedTierForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting",
        "ssm:ResetServiceSetting"
      ],
      "Resource" : "arn:aws:ssm:*:*:servicesetting/ssm/managed-instance/activation-
tier"
    },
    {
      "Sid" : "AllowOperatorToAddTagsToSSMDocument",
      "Effect" : "Allow",
      "Action" : "ssm:AddTagsToResource",
      "Resource" : "arn:aws:ssm:*:*:document/SageMaker-Space*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerSpacesRouterPolicy

Deskripsi: Memberikan izin operasi kunci KMS Sistem yang diperlukan untuk Router Sp SageMaker aces untuk mengaktifkan akses jarak jauh yang aman ke EKS Sp SageMaker aces.

`AmazonSageMakerSpacesRouterPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerSpacesRouterPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 November 2025, 04:34 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerSpacesRouterPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "KMSKeyOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
```

```
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:sagemaker:component" : "amazon-sagemaker-spaces",
          "kms:EncryptionContext:sagemaker:eks-cluster-arn" : "${aws:PrincipalTag/eks-
cluster-arn}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSageMakerTrainingPlanCreateAccess

Deskripsi: Kebijakan Terkelola Amazon ini memberikan izin yang diperlukan untuk membuat dan mengelola R SageMaker encana Pelatihan. Ini memungkinkan pengguna untuk membuat Rencana Pelatihan dan Kapasitas Cadangan, menjelaskan Rencana Pelatihan yang ada, dan melakukan operasi pencarian dan daftar.

`AmazonSageMakerTrainingPlanCreateAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerTrainingPlanCreateAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Desember 2024, 13:21 UTC

- Waktu teredit: 12 Februari 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerTrainingPlanCreateAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingPlan",
        "sagemaker:CreateReservedCapacity",
        "sagemaker:DescribeReservedCapacity"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Sid" : "AddTagsToTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "sagemaker:TaggingAction" : [
            "CreateTrainingPlan",
            "CreateReservedCapacity"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : "sagemaker:DescribeTrainingPlan",
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*"
      ]
    },
    {
      "Sid" : "NonResourceLevelTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:SearchTrainingPlanOfferings",
        "sagemaker:ListTrainingPlans"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListUltraServersByReservedCapacityPermissions",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListUltraServersByReservedCapacity",
      "Resource" : [
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSecurityLakeAdministrator

Deskripsi: Menyediakan akses penuh ke Amazon Security Lake dan layanan terkait yang diperlukan untuk mengelola Security Lake.

`AmazonSecurityLakeAdministrator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSecurityLakeAdministrator` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Mei 2023, 22:04 UTC
- Waktu teredit: 23 Februari 2024, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowActionsWithAnyResource",
      "Effect" : "Allow",
      "Action" : [
        "securitylake:*",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListAccounts",
```

```
        "iam:ListRoles",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsWithAnyResourceViaSecurityLake",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCrawler",
        "glue:StopCrawlerSchedule",
        "lambda:CreateEventSourceMapping",
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:GetDatalakeSettings",
        "events:ListConnections",
        "events:ListApiDestinations",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowManagingSecurityLakeS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketNotification",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketVersioning",
        "s3:PutReplicationConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:ListBucket",
```

```
        "s3:PutObject",
        "s3:GetBucketNotification"
      ],
      "Resource" : "arn:aws:s3:::aws-security-data-lake*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowLambdaCreateFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowLambdaAddPermission",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        },
        "StringEquals" : {
          "lambda:Principal" : "securitylake.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase",
        "glue:CreateTable",
        "glue:GetTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:PutRule",
        "events:DescribeRule",
        "events:CreateApiDestination",
        "events:CreateConnection",
        "events:UpdateConnection",
        "events:UpdateApiDestination",
        "events:DeleteConnection",
        "events:DeleteApiDestination",
        "events:ListTargetsByRule",
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AmazonSecurityLake*",
        "arn:aws:events:*:*:rule/SecurityLake*",
        "arn:aws:events:*:*:api-destination/AmazonSecurityLake*",
        "arn:aws:events:*:*:connection/AmazonSecurityLake*"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSQSActions",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes",
        "sqs:GetQueueURL",
        "sqs:AddPermission",
        "sqs:GetQueueAttributes",
        "sqs:DeleteQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:SecurityLake*",
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsCmkGrantForSecurityLake",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::aws-security-data-lake*"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "GenerateDataKey",
            "RetireGrant",
            "Decrypt"
```

```
        ]
      }
    }
  },
  {
    "Sid" : "AllowEnablingQueryBasedSubscribers",
    "Effect" : "Allow",
    "Action" : [
      "ram:CreateResourceShare",
      "ram:AssociateResourceShare"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLikeIfExists" : {
        "ram:ResourceArn" : [
          "arn:aws:glue:*:*:catalog",
          "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
          "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
        ]
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowConfiguringQueryBasedSubscribers",
    "Effect" : "Allow",
    "Action" : [
      "ram:UpdateResourceShare",
      "ram:GetResourceShares",
      "ram:DisassociateResourceShare",
      "ram:DeleteResourceShare"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ram:ResourceShareName" : "LakeFormation*"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
```

```
    {
      "Sid" : "AllowConfiguringCredentialsForSubscriberNotification",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!connection/
AmazonSecurityLake-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForUpdatingGluePartitionsSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForUpdatingGluePartitionsLambdaArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
```

```
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
            "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCrossRegionReplicationSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeS3ReplicationRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "s3.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCrossRegionReplicationS3Arn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeS3ReplicationRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "s3.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:s3:::aws-security-data-lake*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AllowPassRoleForCustomSourceCrawlerSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "glue.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCustomSourceCrawlerGlueArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "glue.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForSubscriberNotificationSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "events.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:subscriber/*"
        }
```

```
      }
    },
    {
      "Sid" : "AllowPassRoleForSubscriberNotificationEventsArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "events.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:events:*:*:rule/AmazonSecurityLake*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowOnboardingToSecurityLakeDependencies",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/securitylake.amazonaws.com/
AWSServiceRoleForSecurityLake",
        "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
        "arn:aws:iam::*:role/aws-service-role/apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "securitylake.amazonaws.com",
            "lakeformation.amazonaws.com",
            "apidestinations.events.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowRolePolicyActionsforSubscibersandSources",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonSecurityLake*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonSecurityLakePermissionsBoundary"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowRegisterS3LocationInLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PutRolePolicy",
        "iam:GetRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowIAMActionsByResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRolePolicies",
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonSecurityLake*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "S3ReadAccessToSecurityLakes",
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource" : "arn:aws:s3:::aws-security-data-lake-*"
    },
    {
      "Sid" : "S3ReadAccessToSecurityLakeMetastoreObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::security-lake-meta-store-manager-*"
    },
    {
      "Sid" : "S3ResourcelessReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSecurityLakeMetastoreManager

Deskripsi: Kebijakan untuk Amazon SecurityLake meta store manager lambda yang memungkinkan akses ke cloudwatch, S3, Glue dan SQS.

`AmazonSecurityLakeMetastoreManager`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSecurityLakeMetastoreManager` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 23 Januari 2024, 15:26 UTC
- Waktu teredit: 01 April 2024, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowWriteLambdaLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
```

```
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLake*",
        "arn:aws:logs:*:*:/aws/lambda/AmazonSecurityLake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowGlueManage",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:GetTable",
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToReadFromSqs",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMetaDataReadWrite",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMetaDataCleanup",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.avro",
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.metadata.json"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSecurityLakePermissionsBoundary

Deskripsi: Amazon Security Lake membuat peran IAM untuk sumber kustom pihak ketiga untuk menulis data ke danau data dan bagi pelanggan pihak ketiga untuk menggunakan data dari danau data, dan menggunakan kebijakan ini saat membuat peran ini untuk menentukan batas izin mereka.

`AmazonSecurityLakePermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSecurityLakePermissionsBoundary` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2022, 14:11 UTC
- Waktu teredit: 14 Mei 2024, 20:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakePermissionsBoundary`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowActionsForSecurityLake",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyActionsForSecurityLake",
      "Effect" : "Deny",
      "NotAction" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
```

```
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeBucket",
      "Effect" : "Deny",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "NotResource" : [
        "arn:aws:s3:::aws-security-data-lake*"
      ]
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeSQS",
      "Effect" : "Deny",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "NotResource" : "arn:aws:sqs:*:*:AmazonSecurityLake*"
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeKMSS3SQS",
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringNotLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeKMSForS3",
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        },
        "StringNotLikeIfExists" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::aws-security-data-lake*"
          ]
        }
      }
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeKMSForS3SQS",
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:sqs:arn" : "false"
        },
        "StringNotLikeIfExists" : {
          "kms:EncryptionContext:aws:sqs:arn" : [
            "arn:aws:sqs:*:*:AmazonSecurityLake*"
          ]
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSESFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon SES melalui Konsol Manajemen AWS.

`AmazonSESFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSESFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 06 Februari 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ses:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSESReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon SES melalui Konsol Manajemen AWS.

`AmazonSESReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSESReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 14 Mei 2024, 12:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SESReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ses:Get*",
        "ses:List*",
        "ses:BatchGetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSESServiceRolePolicy

Deskripsi: Mengizinkan SES mempublikasikan metrik pemantauan CloudWatch dasar Amazon atas nama sumber daya SES Anda

`AmazonSESServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 21 Mei 2024, 16:02 UTC
- Waktu teredit: 21 Mei 2024, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSESServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutMetricDataToSESCloudWatchNamespaces",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : [
            "AWS/SES",
            "AWS/SES/MailManager",
            "AWS/SES/Addons"
          ]
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSNSFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon SNS melalui. Konsol Manajemen AWS

`AmazonSNSFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSNSFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 24 September 2024, 22:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SNSFullAccess",
      "Effect" : "Allow",
      "Action" : "sns:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SMSAccessViaSNS",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:DescribeVerifiedDestinationNumbers",
        "sms-voice:CreateVerifiedDestinationNumber",
        "sms-voice:SendDestinationNumberVerificationCode",
        "sms-voice:SendTextMessage",
        "sms-voice:DeleteVerifiedDestinationNumber",
        "sms-voice:VerifyDestinationNumber",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:SetTextMessageSpendLimitOverride",
        "sms-voice:DescribeOptedOutNumbers",
        "sms-voice:DeleteOptedOutNumber"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sns.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSNSReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon SNS melalui. Konsol Manajemen AWS

`AmazonSNSReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSNSReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 24 September 2024, 22:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SNSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:GetTopicAttributes",
        "sns:List*",
        "sns:CheckIfPhoneNumberIsOptedOut",
        "sns:GetEndpointAttributes",
```

```
        "sns:GetDataProtectionPolicy",
        "sns:GetPlatformApplicationAttributes",
        "sns:GetSMSAttributes",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SMSAccessViaSNS",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:DescribeVerifiedDestinationNumbers",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribeOptedOutNumbers"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sns.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonsnsPeran

Deskripsi: Kebijakan default untuk peran layanan Amazon SNS.

`AmazonSNSRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSNSRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 06 Februari 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSNSRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSQSFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon SQS melalui. Konsol Manajemen AWS

`AmazonSQSFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSQSFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 06 Februari 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Action" : [
        "sqs:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSQSReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon SQS melalui. Konsol Manajemen AWS

`AmazonSQSReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSQSReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 24 Mei 2024, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSQSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListMessageMoveTasks",
        "sqs:ListQueueTags"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSSMAutomationApproverAccess

Deskripsi: Menyediakan akses untuk melihat eksekusi otomatisasi dan mengirim keputusan persetujuan ke otomatisasi menunggu persetujuan

`AmazonSSMAutomationApproverAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSSMAutomationApproverAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Agustus 2017, 23:07 UTC
- Waktu teredit: 07 Agustus 2017, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationExecutions",
        "ssm:GetAutomationExecution",
        "ssm:SendAutomationSignal"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSSMAutomationRole

Deskripsi: Memberikan izin untuk layanan Otomasi EC2 untuk menjalankan aktivitas yang ditentukan dalam dokumen Otomasi

`AmazonSSMAutomationRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSSMAutomationRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Desember 2016, 22:09 UTC
- Waktu teredit: 20 Maret 2026, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:Automation*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage",
        "ec2:CopyImage",
        "ec2:DeregisterImage",
        "ec2:DescribeImages",
        "ec2:DeleteSnapshot",
        "ec2:StartInstances",
        "ec2:RunInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:*"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:Automation*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:*:ssm:*:*:session/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSSMDirectoryServiceAccess

Deskripsi: Kebijakan ini memungkinkan Agen SSM mengakses Layanan Direktori atas nama pelanggan untuk bergabung dengan domain instans terkelola.

`AmazonSSMDirectoryServiceAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSSMDirectoryServiceAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Maret 2019, 17:44 UTC
- Waktu teredit: 15 Maret 2019, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSSMFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon SSM.

`AmazonSSMFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSSMFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 Mei 2015, 17:39 UTC
- Waktu teredit: 20 November 2019, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
```

```
        "ds:CreateComputer",
        "ds:DescribeDirectories",
        "ec2:DescribeInstanceStatus",
        "logs:*",
        "ssm:*",
        "ec2messages:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSSMMaintenanceWindowRole

Deskripsi: Peran Layanan yang akan digunakan untuk Jendela Pemeliharaan EC2

`AmazonSSMMaintenanceWindowRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSSMMaintenanceWindowRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Desember 2016, 15:57 UTC
- Waktu teredit: 27 Juli 2019, 00:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:GetParameters",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SSM*",
        "arn:aws:lambda:*:*:function:*:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "states:DescribeExecution",
        "states:StartExecution"
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:SSM*",
        "arn:aws:states:*:*:execution:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSSMManagedEC2InstanceDefaultPolicy

Deskripsi: Kebijakan ini mengaktifkan fungsionalitas Manajer AWS Sistem pada instans EC2.

`AmazonSSMManagedEC2InstanceDefaultPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSSMManagedEC2InstanceDefaultPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Agustus 2022, 20:54 UTC
- Waktu teredit: 16 Juli 2024, 18:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSSMAgentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSSMChannelMessaging",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AllowSSMLegacyMessaging",
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSSMManagedInstanceCore

Deskripsi: Kebijakan Amazon EC2 Role untuk mengaktifkan fungsionalitas inti layanan Manajer AWS Sistem.

`AmazonSSMManagedInstanceCore`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSSMManagedInstanceCore` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Maret 2019, 17:22 UTC

- Waktu teredit: 23 Mei 2019, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
```

```
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSSMPatchAssociation

Deskripsi: Menyediakan akses ke instance anak untuk operasi asosiasi patch.

`AmazonSSMPatchAssociation`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSSMPatchAssociation` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 13 Mei 2020, 16:00 UTC
- Waktu teredit: 13 Mei 2020, 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMPatchAssociation`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ssm:DescribeEffectivePatchesForPatchBaseline",
      "Resource" : "arn:aws:ssm:*:*:patchbaseline/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:GetPatchBaseline",
      "Resource" : "arn:aws:ssm:*:*:patchbaseline/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:DescribePatchBaselines",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSSMReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon SSM.

`AmazonSSMReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSSMReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 Mei 2015, 17:44 UTC
- Waktu teredit: 29 Mei 2015, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSSMServiceRolePolicy

Deskripsi: Menyediakan akses ke AWS Sumber Daya yang dikelola atau digunakan oleh Amazon SSM

`AmazonSSMServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 13 November 2017, 19:20 UTC
- Waktu teredit: 26 Juni 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v17 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:GetAutomationExecution",
        "ssm:GetParameters",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:ListTagsForResource",
        "ssm:GetCalendarState",
        "ssm:ListCloudConnectors"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutInventory"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
```

```
          "ssm:InventoryTypeName" : [
            "AWS:ComplianceItem",
            "AWS:PatchSummary"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SSM*",
        "arn:aws:lambda:*:*:function:*:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "states:DescribeExecution",
        "states:StartExecution"
```

```
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:SSM*",
        "arn:aws:states:*:*:execution:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:SelectResourceConfig"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEnrollmentStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeTrustedAdvisorChecks",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeCases"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeComplianceByConfigRule",
        "config:DescribeComplianceByResource",
        "config:DescribeRemediationConfigurations",
        "config:DescribeConfigurationRecorders"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:DescribeAlarms",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:ListStackSets",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackInstances",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:DeleteStackSet"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-SSM*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:DeleteStackInstances",
      "Resource" : [
        "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-SSM*:*",
        "arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-SSM*:*",
        "arn:aws:cloudformation:*:*:type/resource/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "events:ManagedBy" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/SSMExplorerManagedRule"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "events:DescribeRule",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "securityhub:DescribeHub",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-explorer-2:CreateManagedView",
      "Resource" : "arn:aws:resource-explorer-2:*:*:managed-view/AWSManagedViewForSSM*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonSumerianFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Sumerian.

`AmazonSumerianFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSumerianFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 April 2018, 20:14 UTC
- Waktu teredit: 24 April 2018, 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSumerianFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sumerian:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonTextractFullAccess

Deskripsi: Akses ke semua API Amazon Textract

`AmazonTextractFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonTextractFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2018, 19:07 UTC
- Waktu teredit: 28 November 2018, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTextractFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "textract:*"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonTextractServiceRole

Deskripsi: Mengizinkan Textract untuk memang AWS gil layanan atas nama Anda.

`AmazonTextractServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonTextractServiceRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 28 November 2018, 19:12 UTC
- Waktu teredit: 28 November 2018, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonTextractServiceRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:AmazonTextract*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonTimestreamConsoleFullAccess

Deskripsi: Menyediakan akses penuh untuk mengelola Amazon Timestream menggunakan. Konsol Manajemen AWS Perhatikan bahwa kebijakan ini juga memberikan izin untuk operasi KMS tertentu, dan operasi untuk mengelola kueri yang disimpan. Jika menggunakan CMK yang dikelola pelanggan, silakan lihat dokumentasi untuk izin tambahan yang diperlukan.

`AmazonTimestreamConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonTimestreamConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 30 September 2020, 21:47 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v13 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:timestream:database-name"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "timestream.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dbqms:CreateFavoriteQuery",
        "dbqms:DescribeFavoriteQueries",
        "dbqms:UpdateFavoriteQuery",
        "dbqms:DeleteFavoriteQueries",
        "dbqms:GetQueryString",
        "dbqms:CreateQueryHistory",
        "dbqms:DescribeQueryHistory",
        "dbqms:UpdateQueryHistory",
        "dbqms:DeleteQueryHistory"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "iam:ListRoles"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceViewSubscriptions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:AcceptAgreementRequest",
        "aws-marketplace:CreateAgreementRequest",
        "aws-marketplace:ListEntitlementDetails",
        "aws-marketplace:DescribeAgreement",
        "aws-marketplace:Subscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "prod-xcc5llpq4vlbc",
            "prod-5jijo74ujy36m",
            "prod-rjppt7huo35fm"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonTimestreamFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Timestream. Perhatikan bahwa kebijakan ini juga memberikan akses operasi KMS tertentu. Jika menggunakan CMK yang dikelola pelanggan, silakan lihat dokumentasi untuk izin tambahan yang diperlukan.

`AmazonTimestreamFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonTimestreamFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 September 2020, 21:47 UTC
- Waktu teredit: 26 November 2021, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:timestream:database-name"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "timestream.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonTimestreamInfluxDBFullAccess

Deskripsi: Menyediakan akses administratif penuh untuk membuat, memperbarui, menghapus, dan membuat daftar instans Amazon Timestream InfluxDB serta membuat dan membuat daftar grup parameter. Silakan merujuk ke dokumentasi untuk izin tambahan yang diperlukan.

`AmazonTimestreamInfluxDBFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonTimestreamInfluxDBFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Maret 2024, 22:53 UTC
- Waktu teredit: 03 Agustus 2026, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess`

Versi kebijakan

Versi kebijakan: v18 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TimestreamInfluxDBStatement",
      "Effect" : "Allow",
      "Action" : [
        "timestream-influxdb:CreateDbParameterGroup",
        "timestream-influxdb:GetDbParameterGroup",
        "timestream-influxdb:ListDbParameterGroups",
        "timestream-influxdb:CreateDbInstance",
        "timestream-influxdb:DeleteDbInstance",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:TagResource",
        "timestream-influxdb:UntagResource",
        "timestream-influxdb:ListTagsForResource",
        "timestream-influxdb:UpdateDbInstance",
        "timestream-influxdb:CreateDbCluster",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:UpdateDbCluster",
        "timestream-influxdb:DeleteDbCluster",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstancesForCluster",
        "timestream-influxdb:RebootDbInstance",
        "timestream-influxdb:RebootDbCluster",
        "timestream-influxdb:CreateDbBackup",
        "timestream-influxdb:GetDbBackup",
        "timestream-influxdb:ListDbBackups",
        "timestream-influxdb:DeleteDbBackup",
        "timestream-influxdb:RestoreFromDbBackup"
      ],
      "Resource" : "arn:aws:timestream-influxdb:*:*:*"
    },
    {
      "Sid" : "ServiceLinkedRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/timestream-
influxdb.amazonaws.com/AWSServiceRoleForTimestreamInfluxDB",
      "Condition" : {
```

```
        "StringLike" : {
          "iam:AWSServiceName" : "timestream-influxdb.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "NetworkValidationStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BucketValidationStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
```

```
    },
    {
      "Sid" : "MPViewAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MPSubscriptionAccessStatement",
      "Effect" : "Allow",
      "Action" : "aws-marketplace:Subscribe",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "prod-xcc5llpq4vlbc",
            "prod-rjppt7huo35fm"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess

Deskripsi: Menyediakan akses administratif untuk mengelola instans Amazon Timestream InfluxDB dan grup parameter kecuali operasi pasar.

`AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 April 2025, 17:52 UTC
- Waktu teredit: 03 Agustus 2026, 22:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TimestreamInfluxDBStatement",
      "Effect" : "Allow",
      "Action" : [
        "timestream-influxdb:CreateDbParameterGroup",
        "timestream-influxdb:GetDbParameterGroup",
        "timestream-influxdb:ListDbParameterGroups",
        "timestream-influxdb:CreateDbInstance",
        "timestream-influxdb:DeleteDbInstance",
        "timestream-influxdb:GetDbInstance",
```

```
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:TagResource",
        "timestream-influxdb:UntagResource",
        "timestream-influxdb:ListTagsForResource",
        "timestream-influxdb:UpdateDbInstance",
        "timestream-influxdb:CreateDbCluster",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:UpdateDbCluster",
        "timestream-influxdb:DeleteDbCluster",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstancesForCluster",
        "timestream-influxdb:RebootDbInstance",
        "timestream-influxdb:RebootDbCluster",
        "timestream-influxdb:CreateDbBackup",
        "timestream-influxdb:GetDbBackup",
        "timestream-influxdb:ListDbBackups",
        "timestream-influxdb:DeleteDbBackup",
        "timestream-influxdb:RestoreFromDbBackup"
      ],
      "Resource" : [
        "arn:aws:timestream-influxdb:*:*:*"
      ]
    },
    {
      "Sid" : "ServiceLinkedRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/timestream-
influxdb.amazonaws.com/AWSServiceRoleForTimestreamInfluxDB",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "timestream-influxdb.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "NetworkValidationStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BucketValidationStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonTimestreamInfluxDBServiceRolePolicy

Deskripsi: Menyediakan akses administratif penuh untuk membuat, memperbarui, menghapus, dan membuat daftar instans Amazon Timestream InfluxDB serta membuat dan membuat daftar grup parameter. Silakan merujuk ke dokumentasi untuk izin tambahan yang diperlukan.

`AmazonTimestreamInfluxDBServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 14 Maret 2024, 18:53 UTC
- Waktu teredit: 20 Juli 2026, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "CreateEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonTimestreamInfluxDBManaged" : "false"
        }
      }
    },
    {
      "Sid" : "CreateTagWithEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonTimestreamInfluxDBManaged" : "false"
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "ManageEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonTimestreamInfluxDBManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PutCloudWatchMetricsStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Timestream/InfluxDB",
            "AWS/Usage"
          ]
        }
      },
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ManageSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:READONLY-InfluxDB-auth-parameters-*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RetrievePluginSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:InfluxDB-RepoToken-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DecryptPluginSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:*:kms:*:${aws:PrincipalAccount}:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN" :
 "arn:*:secretsmanager:*:*:secret:InfluxDB-RepoToken-*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonTimestreamReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Timestream. Kebijakan juga memberikan izin untuk membatalkan kueri yang sedang berjalan. Jika menggunakan CMK yang dikelola pelanggan, silakan lihat dokumentasi untuk izin tambahan yang diperlukan.

`AmazonTimestreamReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonTimestreamReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 September 2020, 21:47 UTC
- Waktu teredit: 05 Juni 2024, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "AmazonTimestreamReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "timestream:CancelQuery",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:Select",
        "timestream:SelectValues",
        "timestream:DescribeScheduledQuery",
        "timestream:ListScheduledQueries",
        "timestream:DescribeBatchLoadTask",
        "timestream:ListBatchLoadTasks",
        "timestream:DescribeAccountSettings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonTranscribeFullAccess

Deskripsi: Menyediakan akses penuh ke operasi Amazon Transcribe

`AmazonTranscribeFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonTranscribeFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 April 2018, 16:06 UTC
- Waktu teredit: 04 April 2018, 16:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*transcribe*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonTranscribeReadOnlyAccess

Deskripsi: Menyediakan akses ke operasi baca saja untuk Amazon Transcribe

`AmazonTranscribeReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonTranscribeReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 April 2018, 16:05 UTC
- Waktu teredit: 04 April 2018, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:Get*",
        "transcribe:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonVerifiedPermissionsFullAccess

Deskripsi: Menyediakan akses penuh ke Izin Terverifikasi

`AmazonVerifiedPermissionsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonVerifiedPermissionsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Oktober 2024, 18:19 UTC
- Waktu teredit: 11 Oktober 2024, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVerifiedPermissionsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccountLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:CreatePolicyStore",
        "verifiedpermissions:ListPolicyStores"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PolicyStoreLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:*"
      ],
      "Resource" : [
        "arn:aws:verifiedpermissions::*:policy-store/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonVerifiedPermissionsReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke layanan Izin Terverifikasi.

`AmazonVerifiedPermissionsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonVerifiedPermissionsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Oktober 2024, 18:25 UTC
- Waktu teredit: 11 Oktober 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVerifiedPermissionsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccountLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:ListPolicyStores"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "PolicyStoreLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:IsAuthorized",
        "verifiedpermissions:IsAuthorizedWithToken",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicies",
        "verifiedpermissions:ListPolicyTemplates"
      ],
      "Resource" : [
        "arn:aws:verifiedpermissions::*:policy-store/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonVPCCrossAccountNetworkInterfaceOperations

Deskripsi: Menyediakan akses untuk membuat antarmuka jaringan dan melampirkannya ke sumber daya lintas akun

`AmazonVPCCrossAccountNetworkInterfaceOperations`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonVPCCrossAccountNetworkInterfaceOperations` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Juli 2017, 20:47 UTC
- Waktu teredit: 25 September 2023, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRouteTables",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:ReplaceRoute"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
```

```
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonVPCFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon VPC melalui. Konsol Manajemen AWS

`AmazonVPCFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonVPCFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCFullAccess`

Versi kebijakan

Versi kebijakan: v13 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonVPCFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
```

```
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSecurityGroupVpc",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachClassicLinkVpc",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCarrierGateway",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateFlowLogs",
        "ec2:CreateInternetGateway",
        "ec2:CreateLocalGatewayRouteTableVpcAssociation",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpcEndpointConnectionNotification",
        "ec2:CreateVpcEndpointServiceConfiguration",
        "ec2:CreateVpcPeeringConnection",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteCarrierGateway",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteEgressOnlyInternetGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteInternetGateway",
```

```
        "ec2:DeleteLocalGatewayRouteTableVpcAssociation",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpcEndpointConnectionNotifications",
        "ec2:DeleteVpcEndpointServiceConfigurations",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DetachClassicLinkVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLink",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSecurityGroupVpc",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVpcClassicLink",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySecurityGroupRules",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ModifyVpcEndpointConnectionNotification",
        "ec2:ModifyVpcEndpointServiceConfiguration",
        "ec2:ModifyVpcEndpointServicePermissions",
        "ec2:ModifyVpcPeeringConnectionOptions",
        "ec2:ModifyVpcTenancy",
```

```
        "ec2:MoveAddressToVpc",
        "ec2:RejectVpcEndpointConnections",
        "ec2:RejectVpcPeeringConnection",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:ResetNetworkInterfaceAttribute",
        "ec2:RestoreAddressToClassic",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:UnassignIpv6Addresses",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

Deskripsi: Memberikan izin untuk menjelaskan AWS sumber daya, menjalankan Network Access Analyzer, dan membuat atau menghapus tag pada Lingkup Akses Wawasan Jaringan dan Analisis Lingkup Akses Wawasan Jaringan.

`AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonVPCNetworkAccessAnalyzerFullAccessPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Juni 2023, 22:56 UTC
- Waktu teredit: 14 Agustus 2026, 17:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DirectconnectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsAccessScope",
        "ec2:DeleteNetworkInsightsAccessScope",
        "ec2:DeleteNetworkInsightsAccessScopeAnalysis",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:GetTransitGatewayPolicyTableEntries",
        "ec2:GetTransitGatewayPolicyTableAssociations",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeAddresses",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAccessScopeAnalysis"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-insights-access-scope/*",
        "arn:*:ec2:*:*:network-insights-access-scope-analysis/*"
      ]
    },
    {
      "Sid" : "ElasticloadbalancingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlobalacceleratorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallMetadata",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TirosPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tiros:CreateQuery",
        "tiros:GetQueryAnswer"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonVPCReachabilityAnalyzerFullAccessPolicy

Deskripsi: Memberikan izin untuk menjelaskan AWS sumber daya, menjalankan Reachability Analyzer, dan membuat atau menghapus tag pada Jalur Wawasan Jaringan dan Analisis Wawasan Jaringan.

`AmazonVPCReachabilityAnalyzerFullAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonVPCReachabilityAnalyzerFullAccessPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Juni 2023, 20:12 UTC
- Waktu teredit: 14 Agustus 2026, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerFullAccessPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DirectconnectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsPath",
        "ec2:DeleteNetworkInsightsAnalysis",
        "ec2:DeleteNetworkInsightsPath",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
```

```
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:GetTransitGatewayPolicyTableEntries",
        "ec2:GetTransitGatewayPolicyTableAssociations",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeAddresses",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAnalysis"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-insights-path/*",
        "arn:*:ec2:*:*:network-insights-analysis/*"
      ]
    },
    {
      "Sid" : "ElasticloadbalancingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlobalacceleratorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallMetadata",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TirosPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

Deskripsi: Kebijakan ini dilampirkan pada peran IAMRoleForReachabilityAnalyzerCrossAccountResourceAccess. Peran ini diterapkan ke akun anggota dalam organisasi ketika akun manajemen mengaktifkan akses tepercaya untuk Reachability Analyzer. Ini memberikan izin untuk melihat sumber daya dari seluruh organisasi Anda menggunakan konsol Reachability Analyzer.

`AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonVPCReachabilityAnalyzerPathComponentReadPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Mei 2023, 20:38 UTC
- Waktu teredit: 01 Mei 2023, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:Describe*",
        "network-firewall:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonVPCReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon VPC melalui. Konsol Manajemen AWS

`AmazonVPCReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonVPCReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonVPCReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonWorkDocsFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon WorkDocs melalui Konsol Manajemen AWS

`AmazonWorkDocsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkDocsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 April 2020, 23:05 UTC
- Waktu teredit: 16 April 2020, 23.05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonWorkDocsReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon WorkDocs melalui Konsol Manajemen AWS

`AmazonWorkDocsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkDocsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Januari 2020, 23:49 UTC
- Waktu teredit: 08 Januari 2020, 23:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "workdocs:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonWorkMailEventsServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Amazon Ev WorkMail ents

`AmazonWorkMailEventsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 16 April 2019, 16:52 UTC
- Waktu teredit: 16 April 2019, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonWorkMailFullAccess

Deskripsi: Menyediakan akses penuh ke WorkMail, Layanan Direktori, SES, EC2 dan akses baca ke metadata KMS.

`AmazonWorkMailFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkMailFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 21 Desember 2020, 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailFullAccess`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:CheckAlias",
        "ds:CreateAlias",
        "ds:CreateDirectory",
        "ds:CreateIdentityPoolDirectory",
        "ds:DeleteDirectory",
        "ds:DescribeDirectories",
        "ds:GetDirectoryLimits",
        "ds:ListAuthorizedApplications",
        "ds:UnauthorizeApplication",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
```

```
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteVpc",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "route53:ChangeResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "route53:GetHostedZone",
        "route53domains:CheckDomainAvailability",
        "route53domains:ListDomains",
        "ses:*",
        "workmail:*",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "events.workmail.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.workmail.amazonaws.com/
AWSServiceRoleForAmazonWorkMailEvents*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*workmail*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "events.workmail.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonWorkMailMessageFlowFullAccess

Deskripsi: Akses penuh ke API WorkMail Alur Pesan

`AmazonWorkMailMessageFlowFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkMailMessageFlowFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Februari 2021, 11:08 UTC

- Waktu teredit: 11 Februari 2021, 11:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workmailmessageflow:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonWorkMailMessageFlowReadOnlyAccess

Deskripsi: Akses baca saja ke WorkMail pesan untuk GetRawMessageContent API

`AmazonWorkMailMessageFlowReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkMailMessageFlowReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Januari 2021, 12:40 UTC
- Waktu teredit: 28 Januari 2021, 12:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "workmailmessageflow:Get*"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonWorkMailReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke WorkMail dan SES.

`AmazonWorkMailReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkMailReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 25 Juli 2019, 08:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ses:Describe*",
        "ses:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "lambda:ListFunctions",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonWorkSpacesAdmin

Deskripsi: Menyediakan akses ke tindakan WorkSpaces administratif Amazon melalui AWS SDK dan CLI.

`AmazonWorkSpacesAdmin`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkSpacesAdmin` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 September 2015, 22:21 UTC
- Waktu teredit: 27 Juni 2024, 17:16 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonWorkSpacesAdmin",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys",
        "workspaces:CreateTags",
        "workspaces:CreateWorkspaceImage",
        "workspaces:CreateWorkspaces",
        "workspaces:CreateWorkspacesPool",
        "workspaces:CreateStandbyWorkspaces",
        "workspaces:DeleteTags",
        "workspaces:DeregisterWorkspaceDirectory",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:DescribeWorkspaceDirectories",
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspacesPools",
        "workspaces:DescribeWorkspacesPoolSessions",
        "workspaces:DescribeWorkspacesConnectionStatus",
        "workspaces:ModifyCertificateBasedAuthProperties",
        "workspaces:ModifySamlProperties",
        "workspaces:ModifyStreamingProperties",
        "workspaces:ModifyWorkspaceCreationProperties",
        "workspaces:ModifyWorkspaceProperties",
        "workspaces:RebootWorkspaces",
```

```
        "workspaces:RebuildWorkspaces",
        "workspaces:RegisterWorkspaceDirectory",
        "workspaces:RestoreWorkspace",
        "workspaces:StartWorkspaces",
        "workspaces:StartWorkspacesPool",
        "workspaces:StopWorkspaces",
        "workspaces:StopWorkspacesPool",
        "workspaces:TerminateWorkspaces",
        "workspaces:TerminateWorkspacesPool",
        "workspaces:TerminateWorkspacesPoolSession",
        "workspaces:UpdateWorkspacesPool"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonWorkSpacesApplicationManagerAdminAccess

Deskripsi: Menyediakan akses administrator untuk mengemas aplikasi di Amazon WorkSpaces Application Manager.

`AmazonWorkSpacesApplicationManagerAdminAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkSpacesApplicationManagerAdminAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 09 April 2015, 14:03 UTC
- Waktu teredit: 09 April 2015, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesApplicationManagerAdminAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "wam:AuthenticatePackager",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonWorkspacesPCAAccess

Deskripsi: Kebijakan terkelola ini menyediakan akses administratif penuh ke sumber daya CA Pribadi Manajer AWS Sertifikat di oten Akun AWS tikasi berbasis sertifikat Anda.

`AmazonWorkspacesPCAAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkspacesPCAAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 November 2022, 00:25 UTC
- Waktu teredit: 08 November 2022, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "arn:*:acm-pca:*:*:*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/euc-private-ca" : "*"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonWorkSpacesPoolServiceAccess

Deskripsi: Kebijakan ini menyediakan akses AWS WorkSpaces layanan ke sumber daya akun pelanggan yang diperlukan untuk meluncurkan Kolam Ruang Kerja

`AmazonWorkSpacesPoolServiceAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkSpacesPoolServiceAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2024, 16:21 UTC
- Waktu teredit: 27 Juni 2024, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesPoolServiceAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProvisioningWorkSpacesPoolPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "WorkSpacesPoolS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:DeleteObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::wspool-logs-*",
        "arn:aws:s3:::wspool-app-settings-*",
        "arn:aws:s3:::wspool-home-folder-*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonWorkSpacesSecureBrowserReadOnly

Deskripsi: Menyediakan akses baca-saja ke Amazon WorkSpaces Secure Browser dan dependensinya melalui Konsol Manajemen AWS, SDK, dan CLI.

`AmazonWorkSpacesSecureBrowserReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkSpacesSecureBrowserReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2024, 20:01 UTC
- Waktu teredit: 24 Juni 2024, 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSecureBrowserReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkSpacesSecureBrowser",
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserSettings",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetIpAccessSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserSettings",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListIpAccessSettings"
      ],
      "Resource" : "arn:aws:workspaces-web:*:*:*"
    },
    {
      "Sid" : "Dependencies",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
```

```
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonWorkSpacesSelfServiceAccess

Deskripsi: Menyediakan akses ke layanan WorkSpaces backend Amazon untuk melakukan tindakan Layanan Mandiri Workspace

`AmazonWorkSpacesSelfServiceAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkSpacesSelfServiceAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2019, 19:22 UTC
- Waktu teredit: 27 Juni 2019, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces",
        "workspaces:ModifyWorkspaceProperties"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonWorkSpacesServiceAccess

Deskripsi: Menyediakan akses akun pelanggan ke AWS WorkSpaces layanan untuk meluncurkan Workspace.

`AmazonWorkSpacesServiceAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkSpacesServiceAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2019, 19:19 UTC
- Waktu teredit: 18 Maret 2020, 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonWorkSpacesThinClientFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon WorkSpaces Thin Client serta akses terbatas ke layanan terkait yang diperlukan

`AmazonWorkSpacesThinClientFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkSpacesThinClientFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Agustus 2024, 07:25 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesThinClientFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowThinClientFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "thinclient:*"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowWorkSpacesAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowWorkSpacesSecureBrowserAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppStreamAccess",
      "Effect" : "Allow",
      "Action" : [
        "appstream:DescribeStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
monitoring.thinclient.amazonaws.com/
AWSServiceRoleForAmazonWorkSpacesThinClientMonitoring",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "monitoring.thinclient.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonWorkSpacesThinClientMonitoringServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Amazon WorkSpaces Thin Client Monitoring

`AmazonWorkSpacesThinClientMonitoringServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 13 Juni 2025, 19:37 UTC
- Waktu teredit: 13 Juni 2025, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesThinClientMonitoringServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudWatchPutMetricData",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/WorkSpacesThinClient",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonWorkSpacesThinClientReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke Amazon WorkSpaces Thin Client dan dependensinya

`AmazonWorkSpacesThinClientReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkSpacesThinClientReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Juli 2024, 08:50 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesThinClientReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowThinClientReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "thinclient:GetDevice",
        "thinclient:GetDeviceDetails",
        "thinclient:GetEnvironment",
        "thinclient:GetSoftwareSet",
        "thinclient:ListDevices",
        "thinclient:ListDeviceSessions",
        "thinclient:ListEnvironments",
        "thinclient:ListSoftwareSets",
        "thinclient:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowWorkSpacesAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowWorkSpacesSecureBrowserAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppStreamAccess",
      "Effect" : "Allow",
      "Action" : [
        "appstream:DescribeStacks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonWorkSpacesWebReadOnly

Deskripsi: Menyediakan akses baca-saja ke Amazon WorkSpaces Web dan dependensinya melalui Konsol Manajemen AWS, SDK, dan CLI.

`AmazonWorkSpacesWebReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonWorkSpacesWebReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2021, 14:20 UTC
- Waktu teredit: 02 November 2022, 20.20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserSettings",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
```

```
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserSettings",
        "workspaces-web:ListUserAccessLoggingSettings"
      ],
      "Resource" : "arn:aws:workspaces-web:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonWorkSpacesWebServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Amazon WorkSpaces Web

`AmazonWorkSpacesWebServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 30 November 2021, 13:15 UTC
- Waktu teredit: 15 Desember 2022, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/WorkSpacesWebManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "WorkSpacesWebManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/WorkSpacesWebManaged" : "true"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/WorkSpacesWeb",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStreamSummary"
      ],
      "Resource" : "arn:aws:kinesis:*:*:stream/amazon-workspaces-web-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonZocaloFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Zocalo.

`AmazonZocaloFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonZocaloFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 06 Februari 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:*",
        "ds:*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
```

```
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmazonZocaloReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Zocalo

`AmazonZocaloReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonZocaloReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 06 Februari 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AmplifyBackendDeployFullAccess

Deskripsi: Memberikan izin akses penuh Amplify untuk menyebarkan sumber daya backend Amplify (AWS AppSync, Amazon Cognito, Amazon S3, dan layanan terkait lainnya) melalui AWS Cloud Development Kit (CDK)AWS

`AmplifyBackendDeployFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmplifyBackendDeployFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Oktober 2023, 21:32 UTC
- Waktu teredit: 14 November 2024, 19:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CDKPreDeploy",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:GetTemplateSummary",
        "cloudformation:DeleteStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/amplify-*",
        "arn:aws:cloudformation:*:*:stack/CDKToolkit/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyMetadata",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "cloudformation:ListStacks",
        "ssm:DescribeParameters",
        "appsync:GetIntrospectionSchema",
        "amplify:GetBackendEnvironment"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmplifyHotSwappableResources",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetSchemaCreationStatus",
        "appsync:StartSchemaCreation",
        "appsync:UpdateResolver",
        "appsync:ListFunctions",
        "appsync:UpdateFunction",
        "appsync:UpdateApiKey"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmplifyHotSwappableFunctionResource",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode",
        "lambda:GetFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
```

```
      "Resource" : [
        "arn:aws:lambda:*:*:function:amplify-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifySandboxLambdaLogsStreamingListTags",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListTags"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:amplify-*"
      ]
    },
    {
      "Sid" : "AmplifySandboxLambdaLogsStreamingFilterLogEvents",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/amplify-*:*",
        "arn:aws:logs:*:*:log-group:amplify-*:*"
      ]
    },
    {
      "Sid" : "AmplifySchema",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*amplify*",
        "arn:aws:s3:::cdk-*-assets-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "CDKDeploy",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/cdk-*-deploy-role-*-*",
        "arn:aws:iam::*:role/cdk-*-file-publishing-role-*-*",
        "arn:aws:iam::*:role/cdk-*-image-publishing-role-*-*",
        "arn:aws:iam::*:role/cdk-*-lookup-role-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifySSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParametersByPath",
        "ssm:GetParameters",
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amplify/*",
        "arn:aws:ssm:*:*:parameter/cdk-bootstrap/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyModifySSMParam",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
```

```
        "ssm:DeleteParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/amplify/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyDiscoverRDSVpcConfig",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBProxies",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "ec2:DescribeSubnets",
        "rds:DescribeDBSubnetGroups"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:cluster:*",
        "arn:aws:rds:*:*:db-proxy:*",
        "arn:aws:rds:*:*:subgrp:*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AnthropicFullAccess

Deskripsi: Menyediakan akses penuh ke Claude Platform di AWS

`AnthropicFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AnthropicFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 April 2026, 04:57 UTC
- Waktu teredit: 25 September 2026, 20:17 UTC
- ARN: `arn:aws:iam::aws:policy/AnthropicFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AnthropicFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-external-anthropic:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicSubscriptionManagement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "prod-3qbeiztufnva6"
          ]
        }
      }
    },
    {
      "Sid" : "AnthropicSubscriptionView",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicFullEnableFederation",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetOutboundWebIdentityFederationInfo",
        "iam:EnableOutboundWebIdentityFederation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicFullGetToken",
      "Effect" : "Allow",
      "Action" : "sts:GetWebIdentityToken",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "sts:IdentityTokenAudience" : [
            "https://api.anthropic.com",
            "https://platform.claude.com"
          ]
        },
        "StringEquals" : {
```

```
          "aws:CalledViaLast" : "aws-external-anthropic.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AnthropicFullTagToken",
      "Effect" : "Allow",
      "Action" : "sts:TagGetWebIdentityToken",
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicReadOnlyKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AnthropicLimitedAccess

Deskripsi: Menyediakan akses terbatas ke Claude Platform di AWS

`AnthropicLimitedAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AnthropicLimitedAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 April 2026, 04:57 UTC
- Waktu teredit: 02 Oktober 2026, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AnthropicLimitedAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AnthropicLimitedWorkspace",
      "Effect" : "Allow",
      "Action" : [
        "aws-external-anthropic:Get*",
        "aws-external-anthropic:List*",
        "aws-external-anthropic:ArchiveAgent",
        "aws-external-anthropic:ArchiveEnvironment",
        "aws-external-anthropic:ArchiveMemoryStore",
        "aws-external-anthropic:ArchiveSession",
        "aws-external-anthropic:ArchiveVault",
        "aws-external-anthropic:CancelBatchInference",
        "aws-external-anthropic:CountTokens",
        "aws-external-anthropic:CreateAgent",
        "aws-external-anthropic:CreateBatchInference",
        "aws-external-anthropic:CreateEnvironment",
        "aws-external-anthropic:CreateFile",
        "aws-external-anthropic:CreateInference",
        "aws-external-anthropic:CreateMemoryStore",
        "aws-external-anthropic:CreateSession",
```

```
        "aws-external-anthropic:CreateSkill",
        "aws-external-anthropic:CreateVault",
        "aws-external-anthropic:CreateWebhook",
        "aws-external-anthropic:DeleteBatchInference",
        "aws-external-anthropic:DeleteEnvironment",
        "aws-external-anthropic:DeleteFile",
        "aws-external-anthropic:DeleteMemoryStore",
        "aws-external-anthropic:DeleteSession",
        "aws-external-anthropic:DeleteSkill",
        "aws-external-anthropic:DeleteVault",
        "aws-external-anthropic:DeleteWebhook",
        "aws-external-anthropic:ProcessEnvironmentWork",
        "aws-external-anthropic:RotateWebhookSecret",
        "aws-external-anthropic:UpdateAgent",
        "aws-external-anthropic:UpdateEnvironment",
        "aws-external-anthropic:UpdateMemoryStore",
        "aws-external-anthropic:UpdateSession",
        "aws-external-anthropic:UpdateSkill",
        "aws-external-anthropic:UpdateVault",
        "aws-external-anthropic:UpdateWebhook"
      ],
      "Resource" : "arn:aws:aws-external-anthropic:*:*:workspace/*"
    },
    {
      "Sid" : "AnthropicLimitedResourceless",
      "Effect" : "Allow",
      "Action" : [
        "aws-external-anthropic:GetAccountStatus",
        "aws-external-anthropic:CallWithBearerToken",
        "aws-external-anthropic:ListKeys",
        "aws-external-anthropic:GetKey",
        "aws-external-anthropic:CreateUserProfile",
        "aws-external-anthropic:GetUserProfile",
        "aws-external-anthropic:UpdateUserProfile",
        "aws-external-anthropic:ListUserProfiles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicLimitedGetToken",
      "Effect" : "Allow",
      "Action" : "sts:GetWebIdentityToken",
      "Resource" : "*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "sts:IdentityTokenAudience" : [
            "https://api.anthropic.com",
            "https://platform.claude.com"
          ]
        },
        "StringEquals" : {
          "aws:CalledViaLast" : "aws-external-anthropic.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AnthropicLimitedTagToken",
      "Effect" : "Allow",
      "Action" : "sts:TagGetWebIdentityToken",
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicLimitedConsoleAccess",
      "Effect" : "Allow",
      "Action" : "aws-external-anthropic:AssumeConsole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-external-anthropic:Capability" : "developer"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AnthropicReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Claude Platform di AWS

`AnthropicReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AnthropicReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 April 2026, 04:57 UTC
- Waktu teredit: 02 Oktober 2026, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AnthropicReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AnthropicReadOnlyWorkspace",
      "Effect" : "Allow",
      "Action" : [
        "aws-external-anthropic:Get*",
        "aws-external-anthropic:List*"
      ],
      "Resource" : "arn:aws:aws-external-anthropic:*:*:workspace/*"
    },
    {
      "Sid" : "AnthropicReadOnlyResourceless",
      "Effect" : "Allow",
      "Action" : [
        "aws-external-anthropic:GetAccountStatus",
```

```
        "aws-external-anthropic:CallWithBearerToken",
        "aws-external-anthropic:ListKeys",
        "aws-external-anthropic:GetKey",
        "aws-external-anthropic:GetUserProfile",
        "aws-external-anthropic:ListUserProfiles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicReadOnlyKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicReadOnlyGetToken",
      "Effect" : "Allow",
      "Action" : "sts:GetWebIdentityToken",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "sts:IdentityTokenAudience" : [
            "https://api.anthropic.com",
            "https://platform.claude.com"
          ]
        },
        "StringEquals" : {
          "aws:CalledViaLast" : "aws-external-anthropic.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AnthropicReadOnlyTagToken",
      "Effect" : "Allow",
      "Action" : "sts:TagGetWebIdentityToken",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AnthropicSelfHostedEnvironmentAccess

Deskripsi: Menyediakan akses untuk mengoperasikan pelari lingkungan yang di-host sendiri untuk Agen Terkelola Claude

`AnthropicSelfHostedEnvironmentAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AnthropicSelfHostedEnvironmentAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Juni 2026, 17:12 UTC
- Waktu teredit: 12 Juni 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AnthropicSelfHostedEnvironmentAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AnthropicSelfHostedEnvironmentWorkspace",
      "Effect" : "Allow",
      "Action" : [
        "aws-external-anthropic:GetEnvironment",
        "aws-external-anthropic:GetSession",
        "aws-external-anthropic:GetSkill",
        "aws-external-anthropic:ProcessEnvironmentWork",
        "aws-external-anthropic:UpdateSession"
      ],
      "Resource" : "arn:aws:aws-external-anthropic:*:*:workspace/*"
    },
    {
      "Sid" : "AnthropicSelfHostedEnvironmentResourceless",
      "Effect" : "Allow",
      "Action" : [
        "aws-external-anthropic:CallWithBearerToken"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

APIGatewayServiceRolePolicy

Deskripsi: Mengizinkan API Gateway mengelola Sumber AWS Daya terkait atas nama pelanggan.

`APIGatewayServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 20 Oktober 2017, 17:23 UTC
- Waktu teredit: 12 Juli 2021, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
```

```
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/amazon-apigateway-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate",
        "acm:GetCertificate"
      ],
      "Resource" : "arn:aws:acm:*:*:certificate/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterfacePermission",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Owner",
            "VpcLinkId"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "servicediscovery:GetNamespace",
      "Resource" : "arn:aws:servicediscovery:*:*:namespace/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "servicediscovery:GetService",
      "Resource" : "arn:aws:servicediscovery:*:*:service/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AppIntegrationsServiceLinkedRolePolicy

Deskripsi: Memungkinkan AppIntegrations untuk mengelola AppFlow sumber daya dan mempublikasikan data CloudWatch metrik atas nama Anda.

`AppIntegrationsServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 30 September 2022, 19:42 UTC
- Waktu teredit: 30 September 2022 19.42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AppIntegrations"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeConnectorEntity",
        "appflow:ListConnectorEntities"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeConnectorProfiles",
        "appflow:UseConnectorProfile"
      ],
      "Resource" : "arn:aws:appflow:*:*:connector-profile/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DeleteFlow",
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:StartFlow",
        "appflow:StopFlow",
        "appflow:UpdateFlow"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AppIntegrationsManaged" : "true"
        }
      },
      "Resource" : "arn:aws:appflow:*:*:flow/FlowCreatedByAppIntegrations-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:TagResource"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AppIntegrationsManaged"
          ]
        }
```

```
      },
      "Resource" : "arn:aws:appflow:*:*:flow/FlowCreatedByAppIntegrations-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ApplicationAutoScalingForAmazonAppStreamAccess

Deskripsi: Kebijakan untuk mengaktifkan Penskalaan Otomatis Aplikasi untuk Amazon AppStream

`ApplicationAutoScalingForAmazonAppStreamAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ApplicationAutoScalingForAmazonAppStreamAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2017, 21:39 UTC
- Waktu teredit: 06 Februari 2017, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ApplicationAutoScalingForAmazonAppStreamAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh fitur Ekspor Berkelanjutan Layanan Penemuan Aplikasi

`ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 09 Agustus 2018, 20:22 UTC
- Waktu teredit: 13 Agustus 2018, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:UpdateTable",
        "firehose:CreateDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "logs:CreateLogGroup"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    },
    {
      "Action" : [
        "firehose:DeleteDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:UpdateDestination"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:firehose:*:*:deliverystream/aws-application-discovery-
service*"
    },
    {
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:PutBucketLogging",
        "s3:PutEncryptionConfiguration"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::aws-application-discovery-service*"
    },
    {
      "Action" : [
        "s3:GetObject"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::aws-application-discovery-service*/*"
    },
    {
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutRetentionPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose*"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "arn:aws:iam::*:role/AWSApplicationDiscoveryServiceFirehose",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "firehose.amazonaws.com"
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "firehose.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AppRunnerNetworkingServiceRolePolicy

Deskripsi: Men AWS AppRunner gizinkan Jaringan mengelola AWS sumber daya terkait atas nama Anda.

`AppRunnerNetworkingServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 12 Januari 2022, 21:02 UTC
- Waktu teredit: 12 Januari 2022, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AWSAppRunnerManaged"
```

```
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "StringLike" : {
          "aws:RequestTag/AWSAppRunnerManaged" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSAppRunnerManaged" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AppRunnerServiceRolePolicy

Deskripsi: Memungkinkan AWS AppRunner untuk mengelola AWS sumber daya terkait atas nama Anda.

`AppRunnerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 14 Mei 2021, 19:15 UTC
- Waktu teredit: 14 Mei 2021 19.15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/apprunner/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
```

```
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/apprunner/*:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AWSAppRunnerManagedRule*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AppStudioServiceRolePolicy

Deskripsi: Memungkinkan AppStudio untuk mengelola AWS sumber daya terkait atas nama Anda.

`AppStudioServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 10 Juli 2024, 05:01 UTC

- Waktu teredit: 13 Maret 2025, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppStudioServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AppStudioResourcePermissionsForCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/appstudio/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AppStudioResourcePermissionsForSecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
```

```
        "secretsmanager:UpdateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:appstudio-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "IsAppStudioSecret"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/IsAppStudioSecret" : "true"
        }
      }
    },
    {
      "Sid" : "AppStudioResourcePermissionsForManagedSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:appstudio!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "appstudio"
        }
      }
    },
    {
      "Sid" : "AppStudioResourceWritePermissionsForManagedSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:appstudio!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "AppStudioResourcePermissionsForSSO",
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso-directory:DescribeUsers",
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AssuranceServiceRolePolicy

Deskripsi: Memungkinkan AWS Jaminan mengakses sumber daya Anda untuk penilaian kepatuhan dan pengumpulan bukti.

`AssuranceServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran

- Waktu pembuatan: 26 Agustus 2026, 21:07 UTC
- Waktu teredit: 26 Agustus 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AssuranceServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AssuranceComplianceRead",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAdjustmentTypes",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeAutoScalingNotificationTypes",
        "autoscaling:DescribeInstanceRefreshes",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHookTypes",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribeLoadBalancerTargetGroups",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeMetricCollectionTypes",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScalingProcessTypes",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeTerminationPolicyTypes",
        "autoscaling:DescribeTrafficSources",
```

```
        "autoscaling:DescribeWarmPool",
        "bedrock-agentcore:GetAgentCard",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetEvaluator",
        "bedrock-agentcore:GetGateway",
        "bedrock-agentcore:GetGatewayTarget",
        "bedrock-agentcore:GetMemory",
        "bedrock-agentcore:GetOnlineEvaluationConfig",
        "bedrock-agentcore:GetPolicy",
        "bedrock-agentcore:GetPolicyEngine",
        "bedrock-agentcore:GetResourcePolicy",
        "bedrock-agentcore:GetTokenVault",
        "bedrock-agentcore:GetWorkloadIdentity",
        "bedrock-agentcore:ListActors",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimeVersions",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListApiKeyCredentialProviders",
        "bedrock-agentcore:ListBrowserProfiles",
        "bedrock-agentcore:ListBrowserSessions",
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListCodeInterpreterSessions",
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListEvaluators",
        "bedrock-agentcore:ListEvents",
        "bedrock-agentcore:ListGatewayTargets",
        "bedrock-agentcore:ListGateways",
        "bedrock-agentcore:ListMemories",
        "bedrock-agentcore:ListMemoryExtractionJobs",
        "bedrock-agentcore:ListMemoryRecords",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "bedrock-agentcore:ListOnlineEvaluationConfigs",
        "bedrock-agentcore:ListPolicies",
        "bedrock-agentcore:ListPolicyEngines",
        "bedrock-agentcore:ListSessions",
        "bedrock-agentcore:ListTagsForResource",
        "bedrock-agentcore:ListWorkloadIdentities",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentMemory",
```

```
        "bedrock:GetAgentVersion",
        "bedrock:GetCustomModel",
        "bedrock:GetDataSource",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowExecution",
        "bedrock:GetFlowVersion",
        "bedrock:GetFoundationModel",
        "bedrock:GetGuardrail",
        "bedrock:GetIngestionJob",
        "bedrock:GetInvocationStep",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetPrompt",
        "bedrock:GetSession",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgentVersions",
        "bedrock:ListAgents",
        "bedrock:ListAutomatedReasoningPolicies",
        "bedrock:ListBlueprints",
        "bedrock:ListCustomModels",
        "bedrock:ListDataSources",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlowExecutionEvents",
        "bedrock:ListFlowExecutions",
        "bedrock:ListFlowVersions",
        "bedrock:ListFlows",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListIngestionJobs",
        "bedrock:ListInvocationSteps",
        "bedrock:ListInvocations",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListPrompts",
        "bedrock:ListSessions",
        "bedrock:ListTagsForResource",
        "bedrock:ValidateFlowDefinition",
        "cloudformation:GetResource",
        "cloudformation:ListResources",
        "cloudformation:ListStackResources",
```

```
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetQueryResults",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListChannels",
        "cloudtrail:ListDashboards",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudtrail:LookupEvents",
        "cloudtrail:StartQuery",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetrics",
        "config:DescribeComplianceByConfigRule",
        "config:DescribeConfigRules",
        "config:DescribeConfigurationAggregators",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConformancePacks",
        "config:DescribeOrganizationConformancePacks",
        "config:GetComplianceDetailsByConfigRule",
        "config:SelectResourceConfig",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListBackups",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplateVersions",
```

```
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEncryptionControls",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeImages",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeDaemon",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTaskSets",
        "ecs:DescribeTasks",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
```

```
        "ecs:ListDaemons",
        "ecs:ListServices",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "ecs:ListTasks",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeAddonVersions",
        "eks:DescribeCapability",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:DescribePodIdentityAssociation",
        "eks:DescribeUpdate",
        "eks:ListAccessEntries",
        "eks:ListAddons",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListCapabilities",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "eks:ListTagsForResource",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:ListTagsForResource",
        "events:ListTagsForResource",
        "events:DescribeEventBus",
        "guardduty:DescribeOrganizationConfiguration",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFindings",
        "guardduty:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:ListDetectors",
```

```
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatEntitySets",
        "guardduty:ListThreatIntelSets",
        "guardduty:ListTrustedEntitySets",
        "iam:GenerateCredentialReport",
        "iam:GetAccessKeyLastUsed",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetGroupPolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListMFADevices",
        "iam:ListPolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
```

```
        "kms:ListResourceTags",
        "lambda:GetFunction",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:ListAliases",
        "lambda:ListCapacityProviders",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListFunctionUrlConfigs",
        "lambda:ListFunctions",
        "lambda:ListLayerVersions",
        "lambda:ListLayers",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "logs:DescribeDeliveryDestinations",
        "logs:DescribeDeliverySources",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeResourcePolicies",
        "logs:DescribeSubscriptionFilters",
        "logs:FilterLogEvents",
        "logs:GetDataProtectionPolicy",
        "logs:GetQueryResults",
        "logs:StartQuery",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventSubscriptions",
        "rds:ListTagsForResource",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetView",
```

```
        "resource-explorer-2:ListViews",
        "resource-explorer-2:Search",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "securityhub:BatchGetSecurityControls",
        "securityhub:DescribeHub",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindings",
        "securityhub:ListSecurityControlDefinitions",
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ApiGatewayRead",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
```

```
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "OrganizationsTopologyRead",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListParents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AssuranceConfigurationRecorderManagement",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:DescribeConfigurationRecorders",
        "config:PutServiceLinkedConfigurationRecorder"
      ],
      "Resource" : "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForAssurance/*"
    },
    {
      "Sid" : "AWSConfigServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AssurancePolicy",
      "Effect" : "Allow",
      "Action" : [
        "assurance:CreateComment",
        "assurance:DownloadEvidence",
        "assurance:GetAssessment",
        "assurance:GetComment",
        "assurance:GetControl",
        "assurance:GetEnvironment",
        "assurance:GetEvidence",
        "assurance:GetProject",
        "assurance:GetTask",
        "assurance:ListAssessmentAnnotations",
        "assurance:ListAssessments",
        "assurance:ListComments",
        "assurance:ListControls",
        "assurance:ListDiscoveredResources",
        "assurance:ListEnabledFrameworks",
        "assurance:ListEvidence",
        "assurance:ListEvidenceAnnotations",
        "assurance:ListProjects",
        "assurance:ListTasks",
        "assurance:StartResourceDiscovery",
        "assurance:UpdateTask",
        "assurance:UploadEvidence"
      ],
      "Resource" : "arn:*:assurance:*:*:environment/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AuroraDsqlServiceLinkedRolePolicy

Deskripsi: Kebijakan untuk Peran Terkait Layanan Amazon Aurora DSQL

`AuroraDsqlServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 03 Desember 2024, 15:06 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AuroraDsqlServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/AuroraDSQL",
            "AWS/Usage"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AutoScalingConsoleFullAccess

Deskripsi: Menyediakan akses penuh ke Auto Scaling melalui Konsol Manajemen AWS.

`AutoScalingConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AutoScalingConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Januari 2017, 19:43 UTC
- Waktu teredit: 06 Februari 2018, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateKeyPair",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:ImportKeyPair"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
```

```
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListSubscriptions",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AutoScalingConsoleReadOnlyAccess

Deskripsi: Menyediakan akses read-only ke Auto Scaling melalui. Konsol Manajemen AWS

`AutoScalingConsoleReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AutoScalingConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Januari 2017, 19:48 UTC
- Waktu teredit: 12 Januari 2017, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListSubscriptions",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AutoScalingFullAccess

Deskripsi: Menyediakan akses penuh ke Auto Scaling.

`AutoScalingFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AutoScalingFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Januari 2017, 19:31 UTC
- Waktu teredit: 06 Februari 2018, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricAlarm",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcClassicLink"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AutoScalingNotificationAccessRole

Deskripsi: Kebijakan default untuk peran layanan AutoScaling Akses Pemberitahuan.

`AutoScalingNotificationAccessRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AutoScalingNotificationAccessRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 06 Februari 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AutoScalingNotificationAccessRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
```

```
        "sns:Publish"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AutoScalingReadOnlyAccess

Deskripsi: Menyediakan akses read-only ke Auto Scaling.

`AutoScalingReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AutoScalingReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Januari 2017, 19:39 UTC
- Waktu teredit: 12 Januari 2017, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AutoScalingServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Penskalaan Otomatis

`AutoScalingServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 08 Januari 2018, 23:10 UTC
- Waktu teredit: 12 November 2025, 18:19 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachClassicLinkVpc",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateReplaceRootVolumeTask",
        "ec2:CreateFleet",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "ec2:DetachClassicLinkVpc",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:ModifyInstanceAttribute",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2InstanceProfileManagement",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "EC2SpotManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ELBManagement",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Register*",
        "elasticloadbalancing:Deregister*",
        "elasticloadbalancing:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWManagement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "SNSManagement",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridgeRuleManagement",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SystemsManagerParameterManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpcLatticeManagement",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:DeregisterTargets",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListTargets",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:RegisterTargets"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ResourceGroupsManagement",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWS-SSM-Automation-DiagnosisBucketPolicy

Deskripsi: Memberikan izin untuk mengakses bucket SSM Diagnosis S3 untuk diagnosis dan remediasi masalah.

`AWS-SSM-Automation-DiagnosisBucketPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWS-SSM-Automation-DiagnosisBucketPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 November 2024, 23:31 UTC
- Waktu teredit: 15 November 2024, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-Automation-DiagnosisBucketPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*/
${aws:PrincipalAccount}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketWithinOrg",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*/
${aws:PrincipalAccount}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
    },
    {
      "Sid" : "AllowReadOnlyAccessListBucketOnSsmDiagnosisBucketInSameAccount",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "s3:prefix" : "*/${aws:PrincipalAccount}/*"
        }
      }
    },
    {
      "Sid" : "AllowReadOnlyAccessListBucketOnSsmDiagnosisBucketWithinOrg",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        },
        "StringLike" : {
          "s3:prefix" : "*/${aws:PrincipalAccount}/*"
        }
      }
    },
    {
      "Sid" : "AllowGetEncryptionConfigurationOnSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "AllowGetEncryptionConfigurationOnSsmDiagnosisBucketWithinOrg",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy

Deskripsi: Memberikan izin untuk Mendiagnosis masalah dengan layanan SSM dengan menjalankan aktivitas yang ditentukan dalam Dokumen Otomasi, terutama digunakan untuk menjalankan dokumen Otomasi dalam pengaturan lintas wilayah lintas akun dengan memicu otomatisasi anak dalam akun anggota.

`AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 November 2024, 00:01 UTC
- Waktu teredit: 29 Agustus 2026, 00:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions",
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-*UnmanagedEC2*",
        "arn:aws:ssm:*:*:document/AWS-DiagnoseHybridActivationIssues",
```

```
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-*UnmanagedEC2*:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-DiagnoseHybridActivationIssues:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAssumeDiagnosisExecutionRoleWithinAccount",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisAdminRole*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListBucketOnSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy

Deskripsi: Memberikan izin untuk Mendiagnosis masalah dengan layanan SSM dengan menjalankan aktivitas yang ditentukan dalam Dokumen Otomasi, terutama digunakan untuk menjalankan dokumen Otomasi dalam account/region pengaturan target dengan mendiagnosis kesehatan layanan SSM di semua node.

`AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 November 2024, 00:08 UTC
- Waktu teredit: 28 Agustus 2026, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "AllowReadOnlyAccessEC2Resource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeNetworkAcls"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetConsoleOutput",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetConsoleOutput"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationStepExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeActivations",
        "ssm:GetAutomationExecution",
        "ssm:GetServiceSetting"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyAccessIAMResource",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-*UnmanagedEC2*",
        "arn:aws:ssm:*:*:document/AWS-DiagnoseHybridActivationIssues",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-*UnmanagedEC2*:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-DiagnoseHybridActivationIssues:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy

Deskripsi: Memberikan izin untuk akun operasional untuk mendiagnosis node yang tidak dikelola dengan memberikan izin khusus Organisasi yang diperlukan oleh otomatisasi SSM untuk menarik daftar akun anggota dalam root Organisasi guna memicu eksekusi lintas wilayah lintas akun dengan mengizinkan asumsi peran Eksekusi di target. account/region

`AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 November 2024, 00:11 UTC
- Waktu teredit: 16 November 2024, 00:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessOrganization",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeDiagnosisExecutionRoleWithinOrg",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWS-SSM-RemediationAutomation-AdministrationRolePolicy

Deskripsi: Memberikan izin untuk Memperbaiki masalah dengan layanan SSM dengan menjalankan aktivitas yang ditentukan dalam Dokumen Otomasi, terutama digunakan untuk menjalankan dokumen Otomasi dalam pengaturan lintas wilayah lintas akun dengan memicu otomatisasi anak dalam akun anggota.

`AWS-SSM-RemediationAutomation-AdministrationRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWS-SSM-RemediationAutomation-AdministrationRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 November 2024, 00:14 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-AdministrationRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions",
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-OrchestrateUnmanagedEC2Actions",
        "arn:aws:ssm:*:*:document/AWS-RemediateSSMAgent*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-OrchestrateUnmanagedEC2Actions:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RemediateSSMAgent*:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/SystemsManagerManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAssumeRemediationExecutionRoleWithinAccount",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationAdminRole*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
```

```
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListBucketOnSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWS-SSM-RemediationAutomation-ExecutionRolePolicy

Deskripsi: Memberikan izin untuk Memperbaiki masalah dengan layanan SSM dengan menjalankan aktivitas yang ditentukan dalam Dokumen Otomasi, terutama digunakan untuk menjalankan dokumen Otomasi dalam account/region pengaturan target dengan memperbaiki kesehatan layanan SSM di semua node.

`AWS-SSM-RemediationAutomation-ExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWS-SSM-RemediationAutomation-ExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 November 2024, 00:17 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-ExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyAccessEC2Resource",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateVpcEndpointForTaggedSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup"
        }
      }
    },
    {
      "Sid" : "AllowCreateVpcEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "RestrictCreateVpcEndpointForSSMService",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
```

```
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : [
            "com.amazonaws.*.ssm",
            "com.amazonaws.*.ssmmessages",
            "com.amazonaws.*.ec2messages"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingVPCEndpoints::VPCE" :
"VPCEndpoint"
        }
      }
    },
    {
      "Sid" : "RestrictCreateVpcEndpointWithTag",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingVPCEndpoints::VPCE" :
"VPCEndpoint",
          "ec2:CreateAction" : [
            "CreateVpcEndpoint"
          ]
        }
      }
    },
    {
      "Sid" : "AllowModifyVpcAttributeForDns",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Attribute" : [
            "EnableDnsSupport",
```

```
            "EnableDnsHostnames"
          ]
        }
      }
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdateForTaggedResource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup"
        }
      }
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdateWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::SG::Rule" :
"HTTPSAccess"
        }
      }
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdateTagRule",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::SG::Rule" :
"HTTPSAccess",
          "ec2:CreateAction" : [
            "AuthorizeSecurityGroupEgress",
            "AuthorizeSecurityGroupIngress"
          ]
        }
      }
    },
    {
      "Sid" : "AllowCreateSecurityGroupForVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "AllowCreateSecurityGroupWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup"
        }
      }
    },
    {
      "Sid" : "AllowTagCreationForSecurityGroupTags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup",
          "ec2:CreateAction" : [
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-OrchestrateUnmanagedEC2Actions",
        "arn:aws:ssm:*:*:document/AWS-RemediateSSMAgent*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-OrchestrateUnmanagedEC2Actions:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RemediateSSMAgent*:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy

Deskripsi: Memberikan izin untuk akun operasional untuk Memperbaiki node yang tidak dikelola dengan memberikan izin khusus Organisasi yang diperlukan oleh otomatisasi SSM untuk menarik daftar akun anggota dalam root Organisasi guna memicu eksekusi lintas wilayah lintas akun dengan mengizinkan asumsi peran Eksekusi di target. account/region

`AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 November 2024, 00:25 UTC
- Waktu teredit: 16 November 2024, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "AllowReadOnlyAccessOrganization",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeRemediationExecutionRoleWithinOrg",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWS_ ConfigRole

Deskripsi: Kebijakan default untuk peran layanan AWS Config. Menyediakan izin yang diperlukan untuk AWS Config untuk melacak perubahan pada AWS sumber daya Anda.

`AWS_ConfigRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWS_ConfigRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 15 September 2020, 20:30 UTC
- Waktu teredit: 23 September 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWS_ConfigRole`

Versi kebijakan

Versi kebijakan: v73 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigRoleStatementID1",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "access-analyzer:ValidatePolicy",
        "account-access:GetEntitlement",
        "account-access:ListEntitlements",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
```

```
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListTagsForResource",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListForms",
        "amplifyuibuilder:ListThemes",
        "aoss:BatchGetCollection",
        "aoss:BatchGetCollectionGroup",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollectionGroups",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListTagsForResource",
        "aoss:ListVpcEndpoints",
        "apigateway:GET",
        "app-integrations:GetApplication",
        "app-integrations:GetDataIntegration",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListApplications",
        "app-integrations:ListDataIntegrations",
        "app-integrations:ListEventIntegrationAssociations",
        "app-integrations:ListEventIntegrations",
        "app-integrations:ListTagsForResource",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
```

```
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExperimentDefinition",
        "appconfig:GetExtension",
        "appconfig:GetExtensionAssociation",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExperimentDefinitions",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListExtensions",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlow",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServices",
        "application-signals:ListTagsForResource",
        "applicationinsights:DescribeApplication",
        "applicationinsights:DescribeComponent",
        "applicationinsights:DescribeLogPattern",
        "applicationinsights:ListApplications",
        "applicationinsights:ListComponents",
        "applicationinsights:ListLogPatterns",
        "applicationinsights:ListLogPatternSets",
        "applicationinsights:ListTagsForResource",
        "appmesh:DescribeGatewayRoute",
        "appmesh:DescribeMesh",
        "appmesh:DescribeRoute",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:DescribeVirtualRouter",
        "appmesh:DescribeVirtualService",
        "appmesh:ListGatewayRoutes",
```

```
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListTagsForResource",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appstream:DescribeAppBlockBuilders",
        "appstream:DescribeAppBlocks",
        "appstream:DescribeApplications",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeFleets",
        "appstream:DescribeImageBuilders",
        "appstream:DescribeStacks",
        "appstream:ListAssociatedFleets",
        "appstream:ListAssociatedStacks",
        "appstream:ListTagsForResource",
        "appsync:GetApi",
        "appsync:GetApiAssociation",
        "appsync:GetApiCache",
        "appsync:GetChannelNamespace",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
        "appsync:GetGraphqlApi",
        "appsync:GetResolver",
        "appsync:GetSourceApiAssociation",
        "appsync:ListApis",
        "appsync:ListChannelNamespaces",
        "appsync:ListDataSources",
        "appsync:ListDomainNames",
        "appsync:ListGraphqlApis",
        "appsync:ListResolvers",
        "appsync:ListSourceApiAssociations",
```

```
        "appsync:ListTagsForResource",
        "appsync:ListTypes",
        "apptest:GetTestCase",
        "apptest:ListTagsForResource",
        "apptest:ListTestCases",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeAnomalyDetector",
        "aps:DescribeLoggingConfiguration",
        "aps:DescribeQueryLoggingConfiguration",
        "aps:DescribeResourcePolicy",
        "aps:DescribeRuleGroupsNamespace",
        "aps:DescribeScraper",
        "aps:DescribeScraperLoggingConfiguration",
        "aps:DescribeWorkspace",
        "aps:DescribeWorkspaceConfiguration",
        "aps:ListAnomalyDetectors",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListScrapers",
        "aps:ListTagsForResource",
        "aps:ListWorkspaces",
        "arc-region-switch:GetPlan",
        "arc-region-switch:ListPlans",
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListTagsForResource",
        "arc-zonal-shift:GetAutoshiftObserverNotificationStatus",
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListDataCatalogs",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:GetAssessmentFramework",
        "auditmanager:GetControl",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessments",
        "auditmanager:ListControls",
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
```

```
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "b2bi:GetCapability",
        "b2bi:GetPartnership",
        "b2bi:GetProfile",
        "b2bi:GetTransformer",
        "b2bi:ListCapabilities",
        "b2bi:ListPartnerships",
        "b2bi:ListProfiles",
        "b2bi:ListTagsForResource",
        "b2bi:ListTransformers",
        "backup-gateway:GetHypervisor",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:DescribeBackupVault",
        "backup:DescribeFramework",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeReportPlan",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:GetTieringConfiguration",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListFrameworks",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListReportPlans",
        "backup:ListRestoreTestingPlans",
        "backup:ListRestoreTestingSelections",
        "backup:ListTags",
        "backup:ListTieringConfigurations",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeConsumableResource",
        "batch:DescribeJobDefinitions",
        "batch:DescribeJobQueues",
```

```
        "batch:DescribeQuotaShare",
        "batch:DescribeSchedulingPolicies",
        "batch:DescribeServiceEnvironments",
        "batch:ListConsumableResources",
        "batch:ListQuotaShares",
        "batch:ListSchedulingPolicies",
        "batch:ListTagsForResource",
        "bcm-dashboards:GetDashboard",
        "bcm-dashboards:ListDashboards",
        "bcm-dashboards:ListTagsForResource",
        "bcm-data-exports:GetExport",
        "bcm-data-exports:ListExports",
        "bcm-data-exports:ListTagsForResource",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetApiKeyCredentialProvider",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetBrowserProfile",
        "bedrock-agentcore:GetCodeInterpreter",
        "bedrock-agentcore:GetConfigurationBundle",
        "bedrock-agentcore:GetEvaluator",
        "bedrock-agentcore:GetGateway",
        "bedrock-agentcore:GetGatewayTarget",
        "bedrock-agentcore:GetMemory",
        "bedrock-agentcore:GetOauth2CredentialProvider",
        "bedrock-agentcore:GetOnlineEvaluationConfig",
        "bedrock-agentcore:GetPaymentConnector",
        "bedrock-agentcore:GetPaymentCredentialProvider",
        "bedrock-agentcore:GetPaymentManager",
        "bedrock-agentcore:GetPolicy",
        "bedrock-agentcore:GetPolicyEngine",
        "bedrock-agentcore:GetPolicyEngineSummary",
        "bedrock-agentcore:GetPolicyGeneration",
        "bedrock-agentcore:GetPolicyGenerationSummary",
        "bedrock-agentcore:GetPolicySummary",
        "bedrock-agentcore:GetResourcePolicy",
        "bedrock-agentcore:GetTokenVault",
        "bedrock-agentcore:GetWorkloadIdentity",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListApiKeyCredentialProviders",
        "bedrock-agentcore:ListBrowserProfiles",
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListCodeInterpreters",
```

```
        "bedrock-agentcore:ListConfigurationBundles",
        "bedrock-agentcore:ListEvaluators",
        "bedrock-agentcore:ListGateways",
        "bedrock-agentcore:ListGatewayTargets",
        "bedrock-agentcore:ListMemories",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "bedrock-agentcore:ListOnlineEvaluationConfigs",
        "bedrock-agentcore:ListPaymentConnectors",
        "bedrock-agentcore:ListPaymentCredentialProviders",
        "bedrock-agentcore:ListPaymentManagers",
        "bedrock-agentcore:ListPolicies",
        "bedrock-agentcore:ListPolicyEngines",
        "bedrock-agentcore:ListPolicyEngineSummaries",
        "bedrock-agentcore:ListPolicyGenerations",
        "bedrock-agentcore:ListPolicyGenerationSummaries",
        "bedrock-agentcore:ListPolicySummaries",
        "bedrock-agentcore:ListTagsForResource",
        "bedrock-agentcore:ListWorkloadIdentities",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAutomatedReasoningPolicy",
        "bedrock:GetBlueprint",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataSource",
        "bedrock:GetEvaluationJob",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetFoundationModel",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetPromptRouter",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListAutomatedReasoningPolicies",
        "bedrock:ListBlueprints",
```

```
        "bedrock:ListDataAutomationProjects",
        "bedrock:ListDataSources",
        "bedrock:ListEnforcedGuardrailsConfiguration",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlows",
        "bedrock:ListFlowVersions",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListPromptRouters",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "billing:GetBillingView",
        "billing:ListBillingViews",
        "billing:ListSourceViewsForBillingView",
        "billing:ListTagsForResource",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListTagsForResource",
        "braket:ListTagsForResource",
        "braket:SearchSpendingLimits",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ViewBudget",
        "cases:BatchGetCaseRule",
        "cases:BatchGetField",
        "cases:GetDomain",
        "cases:GetLayout",
        "cases:GetTemplate",
        "cases:ListCaseRules",
        "cases:ListDomains",
        "cases:ListFields",
        "cases:ListLayouts",
        "cases:ListTemplates",
        "cassandra:Select",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetAnomalyMonitors",
```

```
        "ce:GetAnomalySubscriptions",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "chime:DescribeAppInstance",
        "chime:DescribeAppInstanceBot",
        "chime:DescribeAppInstanceUser",
        "chime:DescribeChannelFlow",
        "chime:ListAppInstanceBots",
        "chime:ListAppInstances",
        "chime:ListChannelFlows",
        "chime:ListTagsForResource",
        "cleanrooms-ml:GetConfiguredModelAlgorithm",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListConfiguredModelAlgorithms",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListTagsForResource",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribePublisher",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeType",
```

```
        "cloudformation:GetResource",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:ListChangeSets",
        "cloudformation:ListResources",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
        "cloudformation:ListTypes",
        "cloudfront:DescribeFunction",
        "cloudfront:DescribeKeyValueStore",
        "cloudfront:GetAnycastIpList",
        "cloudfront:GetCachePolicy",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetConnectionGroup",
        "cloudfront:GetContinuousDeploymentPolicy",
        "cloudfront:GetDistributionTenant",
        "cloudfront:GetFunction",
        "cloudfront:GetKeyGroup",
        "cloudfront:GetMonitoringSubscription",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetOriginRequestPolicy",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:GetVpcOrigin",
        "cloudfront:ListAnycastIpLists",
        "cloudfront:ListCachePolicies",
        "cloudfront:ListCloudFrontOriginAccessIdentities",
        "cloudfront:ListConnectionGroups",
        "cloudfront:ListContinuousDeploymentPolicies",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListFunctions",
        "cloudfront:ListKeyGroups",
        "cloudfront:ListKeyValueStores",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListOriginRequestPolicies",
        "cloudfront:ListPublicKeys",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudfront:ListVpcOrigins",
```

```
        "cloudtrail:DescribeTrails",
        "cloudTrail:GetChannel",
        "cloudtrail:GetDashboard",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetResourcePolicy",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudTrail:ListChannels",
        "cloudtrail:ListDashboards",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:DescribeInsightRules",
        "cloudwatch:GetAlarmMuteRule",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListAlarmMuteRules",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListManagedInsightRules",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackageGroup",
        "codeartifact:DescribeRepository",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListAllowedRepositoriesForGroup",
        "codeartifact:ListDomains",
        "codeartifact:ListPackageGroups",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetFleets",
        "codebuild:BatchGetReportGroups",
        "codebuild:ListFleets",
        "codebuild:ListReportGroups",
        "codebuild:ListSourceCredentials",
```

```
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListRepositories",
        "codecommit:ListTagsForResource",
        "codeconnections:GetConnection",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codedeploy:GetDeploymentConfig",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "codepipeline:ListWebhooks",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:ListConnections",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListTagsForResource",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:AdminGetUser",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeManagedLoginBranding",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeTerms",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetLogDeliveryConfiguration",
        "cognito-idp:GetUICustomization",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
```

```
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListTerms",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "comprehend:DescribeFlywheel",
        "comprehend:ListFlywheels",
        "comprehend:ListTagsForResource",
        "config:BatchGet*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:Put*",
        "config:Select*",
        "connect-campaigns:DescribeCampaign",
        "connect-campaigns:ListCampaigns",
        "connect:DescribeAgentStatus",
        "connect:DescribeDataTable",
        "connect:DescribeEmailAddress",
        "connect:DescribeEvaluationForm",
        "connect:DescribeHoursOfOperation",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribeMetric",
        "connect:DescribeNotification",
        "connect:DescribePhoneNumber",
        "connect:DescribePredefinedAttribute",
        "connect:DescribePrompt",
        "connect:DescribeQueue",
        "connect:DescribeQuickConnect",
        "connect:DescribeRoutingProfile",
        "connect:DescribeRule",
        "connect:DescribeSecurityProfile",
        "connect:DescribeTrafficDistributionGroup",
        "connect:DescribeUser",
        "connect:DescribeUserHierarchyGroup",
        "connect:DescribeUserHierarchyStructure",
        "connect:DescribeView",
        "connect:DescribeWorkspace",
        "connect:GetTaskTemplate",
        "connect:ListAgentStatuses",
        "connect:ListApprovedOrigins",
        "connect:ListDataTables",
```

```
        "connect:ListEvaluationForms",
        "connect:ListEvaluationFormVersions",
        "connect:ListHoursOfOperationOverrides",
        "connect:ListHoursOfOperations",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListMetrics",
        "connect:ListNotifications",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "connect:ListPredefinedAttributes",
        "connect:ListPrompts",
        "connect:ListQueueEmailAddresses",
        "connect:ListQueueQuickConnects",
        "connect:ListQueues",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileManualAssignmentQueues",
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListSecurityProfileAIAgents",
        "connect:ListSecurityProfileApplications",
        "connect:ListSecurityProfileFlowModules",
        "connect:ListSecurityProfilePermissions",
        "connect:ListSecurityProfiles",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListTrafficDistributionGroups",
        "connect:ListUserHierarchyGroups",
        "connect:ListUsers",
        "connect:ListViews",
        "connect:ListViewVersions",
        "connect:ListWorkspaceMedia",
        "connect:ListWorkspacePages",
        "connect:ListWorkspaces",
        "connect:SearchAvailablePhoneNumbers",
        "connect:SearchWorkspaceAssociations",
        "controltower:GetLandingZone",
        "controltower:ListLandingZones",
        "cur:DescribeReportDefinitions",
        "cur:ListTagsForResource",
```

```
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "databrew:ListTagsForResource",
        "datasync:DescribeAgent",
        "datasync:DescribeLocationAzureBlob",
        "datasync:DescribeLocationEfs",
        "datasync:DescribeLocationFsxLustre",
        "datasync:DescribeLocationFsxOntap",
        "datasync:DescribeLocationFsxOpenZfs",
        "datasync:DescribeLocationFsxWindows",
        "datasync:DescribeLocationHdfs",
        "datasync:DescribeLocationNfs",
        "datasync:DescribeLocationObjectStorage",
        "datasync:DescribeLocationS3",
        "datasync:DescribeLocationSmb",
        "datasync:DescribeTask",
        "datasync:ListAgents",
        "datasync:ListLocations",
        "datasync:ListTagsForResource",
        "datasync:ListTasks",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentProfile",
        "datazone:GetGroupProfile",
        "datazone:GetSubscriptionTarget",
        "datazone:GetUserProfile",
        "datazone:ListDomains",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurations",
```

```
        "datazone:ListEnvironmentProfiles",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListSubscriptionTargets",
        "datazone:SearchGroupProfiles",
        "datazone:SearchUserProfiles",
        "dax:DescribeClusters",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "deadline:GetBudget",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetJob",
        "deadline:GetLicenseEndpoint",
        "deadline:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetQueueLimitAssociation",
        "deadline:GetStorageProfile",
        "deadline:ListBudgets",
        "deadline:ListFarms",
        "deadline:ListFleets",
        "deadline:ListJobs",
        "deadline:ListLicenseEndpoints",
        "deadline:ListMonitors",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListQueueLimitAssociations",
        "deadline:ListQueues",
        "deadline:ListStorageProfiles",
        "deadline:ListTagsForResource",
        "deadline:SearchJobs",
        "detective:ListGraphs",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListNetworkProfiles",
```

```
        "devicefarm:ListProjects",
        "devicefarm:ListTagsForResource",
        "devicefarm:ListTestGridProjects",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListNotificationChannels",
        "directconnect:DescribeConnections",
        "dms:DescribeCertificates",
        "dms:DescribeDataMigrations",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationConfigs",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTasks",
        "dms:ListDataProviders",
        "dms:ListInstanceProfiles",
        "dms:ListMigrationProjects",
        "dms:ListTagsForResource",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:ListTagsForResource",
        "ds:DescribeDirectories",
        "ds:DescribeDomainControllers",
        "ds:DescribeEventTopics",
        "ds:ListLogSubscriptions",
        "ds:ListTagsForResource",
        "dsql:GetCluster",
        "dsql:GetClusterPolicy",
        "dsql:GetVpcEndpointServiceName",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
```

```
        "ec2:Describe*",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeTransitGatewayMeteringPolicies",
        "ec2:GetAllowedImagesSettings",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetRouteServerAssociations",
        "ec2:GetRouteServerPropagations",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:SearchTransitGatewayRoutes",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribePullThroughCacheRules",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:DescribeRepositoryCreationTemplates",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:GetRepositoryPolicy",
        "ecr:ListTagsForResource",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeExpressGatewayService",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListServices",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitionFamilies",
```

```
        "ecs:ListTaskDefinitions",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeCapability",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:ListAddons",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListCapabilities",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "eks:ListTagsForResource",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:DescribeCapacityReservation",
        "elasticloadbalancing:DescribeListenerAttributes",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
```

```
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "elemental-inference:GetFeed",
        "elemental-inference:ListFeeds",
        "elemental-inference:ListTagsForResource",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "entityresolution:GetIdMappingWorkflow",
        "entityresolution:GetIdNamespace",
        "entityresolution:GetMatchingWorkflow",
        "entityresolution:GetSchemaMapping",
        "entityresolution:ListIdMappingWorkflows",
```

```
        "entityresolution:ListIdNamespaces",
        "entityresolution:ListMatchingWorkflows",
        "entityresolution:ListSchemaMappings",
        "entityresolution:ListTagsForResource",
        "es:DescribeDomain",
        "es:DescribeDomains",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:GetCompatibleElasticsearchVersions",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListTags",
        "events:DescribeApiDestination",
        "events:DescribeArchive",
        "events:DescribeConnection",
        "events:DescribeEndpoint",
        "events:DescribeEventBus",
        "events:DescribeRule",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "finspace:GetEnvironment",
        "finspace:ListEnvironments",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "firehose:ListTagsForDeliveryStream",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:ListExperimentTemplates",
        "fis:ListTagsForResource",
        "fis:ListTargetAccountConfigurations",
        "fms:GetNotificationChannel",
```

```
        "fms:GetPolicy",
        "fms:ListPolicies",
        "fms:ListTagsForResource",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasets",
        "forecast:ListTagsForResource",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListTagsForResource",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeFileSystems",
        "fsx:DescribeS3AccessPointAttachments",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "gamelift:DescribeAlias",
        "gamelift:DescribeBuild",
        "gamelift:DescribeContainerFleet",
        "gamelift:DescribeContainerGroupDefinition",
        "gamelift:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScalingPolicies",
```

```
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListContainerFleets",
        "gamelift:ListContainerGroupDefinitions",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListLocations",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "gamelift:ValidateMatchmakingRuleSet",
        "gameliftstreams:GetApplication",
        "gameliftstreams:GetStreamGroup",
        "gameliftstreams:ListApplications",
        "gameliftstreams:ListStreamGroups",
        "gameliftstreams:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeKey",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListKeys",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeAcceleratorAttributes",
        "globalaccelerator:DescribeCrossAccountAttachment",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCrossAccountAttachments",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
```

```
        "glue:DescribeIntegrations",
        "glue:GetBlueprint",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetRegistry",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetSession",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetWorkflow",
        "glue:ListBlueprints",
        "glue:ListCrawlers",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "glue:ListSessions",
        "glue:ListTriggers",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetComponent",
        "greengrass:GetDeployment",
        "greengrass:ListComponents",
```

```
        "greengrass:ListComponentVersions",
        "greengrass:ListDeployments",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:ListConfigs",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
        "groundstation:ListTagsForResource",
        "guardduty:DescribePublishingDestination",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:GetIPSet",
        "guardduty:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatEntitySet",
        "guardduty:GetThreatIntelSet",
        "guardduty:GetTrustedEntitySet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMalwareProtectionPlans",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatEntitySets",
        "guardduty:ListThreatIntelSets",
        "guardduty:ListTrustedEntitySets",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:GetDataTransformationProfile",
        "healthlake:ListDataTransformationProfiles",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListTagsForResource",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
```

```
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListInstanceProfilesForRole",
        "iam:ListInstanceProfileTags",
        "iam:ListMFADevices",
        "iam:ListMFADeviceTags",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
```

```
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:GetWorkflow",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "imagebuilder:ListLifecyclePolicies",
        "imagebuilder:ListWorkflowBuildVersions",
        "imagebuilder:ListWorkflows",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetCodeSecurityScanConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListCodeSecurityScanConfigurations",
        "inspector2:ListFilters",
        "inspector2:ListMembers",
        "inspector2:ListTagsForResource",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "invoicing:ListProcurementPortalPreferences",
        "invoicing:ListTagsForResource",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeBillingGroup",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCertificateProvider",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJob",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
```

```
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:DescribeStream",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:GetCommand",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:GetV2LoggingOptions",
        "iot:ListAuthorizers",
        "iot:ListBillingGroups",
        "iot:ListCACertificates",
        "iot:ListCertificateProviders",
        "iot:ListCertificates",
        "iot:ListCommands",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "iot:ListPackages",
        "iot:ListPackageVersions",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListThingGroups",
        "iot:ListThingTypes",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:ValidateSecurityProfileBehaviors",
        "iotanalytics:DescribeChannel",
        "iotanalytics:DescribeDataset",
        "iotanalytics:DescribeDatastore",
```

```
        "iotanalytics:DescribePipeline",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotanalytics:ListTagsForResource",
        "iotdeviceadvisor:GetSuiteDefinition",
        "iotdeviceadvisor:ListSuiteDefinitions",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotfleethub:DescribeApplication",
        "iotfleethub:ListApplications",
        "iotfleetwise:GetCampaign",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetStateTemplate",
        "iotfleetwise:GetVehicle"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSConfigRoleStatementID2",
      "Effect" : "Allow",
      "Action" : [
        "iotfleetwise:ListCampaigns",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListStateTemplates",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotsitewise:DescribeAccessPolicy",
```

```
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeComputationModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeDataset",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModelCompositeModels",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:ListComputationModels",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListDatasets",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:GetEntity",
        "iottwinmaker:GetScene",
        "iottwinmaker:GetSyncJob",
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListTagsForResource",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessDeviceImportTask",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
```

```
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListDevicesForWirelessDeviceImportTask",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDeviceImportTasks",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGateways",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:GetChannel",
        "ivs:GetComposition",
        "ivs:GetEncoderConfiguration",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStorageConfiguration",
        "ivs:GetStreamKey",
        "ivs:ListChannels",
        "ivs:ListCompositions",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:DescribeVpcConnection",
        "kafka:GetClusterPolicy",
```

```
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurations",
        "kafka:ListScramSecrets",
        "kafka:ListTagsForResource",
        "kafka:ListVpcConnections",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListTagsForResource",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra-ranking:DescribeRescoreExecutionPlan",
        "kendra-ranking:ListRescoreExecutionPlans",
        "kendra-ranking:ListTagsForResource",
        "kendra:DescribeIndex",
        "kendra:ListDataSources",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:GetResourcePolicy",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lakeformation:DescribeLakeFormationIdentityCenterConfiguration",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
```

```
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionScalingConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:ListAliases",
        "lambda:ListCapacityProviders",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListFunctions",
        "lambda:ListFunctionUrlConfigs",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "launchwizard:GetDeployment",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListTagsForResource",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
        "lex:ListBotAliases",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListDistributedGrants",
```

```
        "license-manager:ListLicenses",
        "license-manager:ListReceivedGrants",
        "license-manager:ListTagsForResource",
        "lightsail:GetActiveNames",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetOperations",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeAccountPolicies",
        "logs:DescribeDeliveries",
        "logs:DescribeDeliveryDestinations",
        "logs:DescribeDeliverySources",
        "logs:DescribeDestinations",
        "logs:DescribeIndexPolicies",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeResourcePolicies",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
```

```
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetIntegration",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:ListIntegrations",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:ListTagsForResource",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:GetEnvironment",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsFilter",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListAllowLists",
        "macie2:ListAutomatedDiscoveryAccounts",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindingsFilters",
        "macie2:ListTagsForResource",
        "managedblockchain:GetAccessor",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:ListAccessors",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
```

```
        "managedblockchain:ListNodes",
        "mediaconnect:DescribeBridge",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeGateway",
        "mediaconnect:GetRouterInput",
        "mediaconnect:GetRouterNetworkInterface",
        "mediaconnect:ListBridges",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGateways",
        "mediaconnect:ListRouterInputs",
        "mediaconnect:ListRouterNetworkInterfaces",
        "mediaconnect:ListRouterOutputs",
        "mediaconnect:ListTagsForResource",
        "medialive:DescribeChannelPlacementGroup",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeNode",
        "medialive:DescribeSdiSource",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:ListChannelPlacementGroups",
        "medialive:ListCloudWatchAlarmTemplateGroups",
        "medialive:ListCloudWatchAlarmTemplates",
        "medialive:ListEventBridgeRuleTemplateGroups",
        "medialive:ListEventBridgeRuleTemplates",
        "medialive:ListMultiplexes",
        "medialive:ListMultiplexPrograms",
        "medialive:ListNodes",
        "medialive:ListSdiSources",
        "medialive:ListSignalMaps",
        "medialive:ListTagsForResource",
        "mediapackage-vod:DescribeAsset",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListAssets",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
```

```
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediatailor:DescribeChannel",
        "mediatailor:DescribeLiveSource",
        "mediatailor:DescribeSourceLocation",
        "mediatailor:DescribeVodSource",
        "mediatailor:GetChannelPolicy",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListChannels",
        "mediatailor:ListLiveSources",
        "mediatailor:ListPlaybackConfigurations",
        "mediatailor:ListSourceLocations",
        "mediatailor:ListVodSources",
        "medical-imaging:GetDatastore",
        "medical-imaging:ListDatastores",
        "medical-imaging:ListTagsForResource",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListTags",
        "mobiletargeting:GetApp",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetCampaign",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetEmailChannel",
        "mobiletargeting:GetEmailTemplate",
        "mobiletargeting:GetEventStream",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:GetSegment",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTagsForResource",
        "mobiletargeting:ListTemplates",
        "mpa:GetIdentitySource",
        "mpa:ListIdentitySources",
        "mpa:ListTagsForResource",
        "mq:DescribeBroker",
        "mq:DescribeConfiguration",
```

```
        "mq:ListBrokers",
        "mq:ListConfigurations",
        "mq:ListTags",
        "neptune-graph:GetGraphSnapshot",
        "neptune-graph:ListGraphSnapshots",
        "neptune-graph:ListTagsForResource",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetDirectConnectGatewayAttachment",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:ListAttachments",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListCoreNetworks",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStudioComponents",
        "nimble:ListStudios",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:ListTagsForResource",
        "notifications:GetEventRule",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
```

```
        "notifications:ListOrganizationalUnits",
        "notifications:ListTagsForResource",
        "nova-act:GetWorkflowDefinition",
        "nova-act:ListWorkflowDefinitions",
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListLinks",
        "oam:ListSinks",
        "oam:ListTagsForResource",
        "omics:GetAnnotationStore",
        "omics:GetConfiguration",
        "omics:GetReferenceStore",
        "omics:GetRun",
        "omics:GetRunCache",
        "omics:GetRunGroup",
        "omics:GetS3AccessPolicy",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:GetWorkflowVersion",
        "omics:ListAnnotationStores",
        "omics:ListConfigurations",
        "omics:ListReferenceStores",
        "omics:ListRunCaches",
        "omics:ListRunGroups",
        "omics:ListRuns",
        "omics:ListSequenceStores",
        "omics:ListTagsForResource",
        "omics:ListVariantStores",
        "omics:ListWorkflows",
        "omics:ListWorkflowVersions",
        "opsworks:DescribeInstances",
        "opsworks:DescribeLayers",
        "opsworks:DescribeTimeBasedAutoScaling",
        "opsworks:DescribeVolumes",
        "opsworks:ListTags",
        "organizations:DescribeAccount",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy",
        "organizations:ListAccounts",
```

```
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "osis:GetPipeline",
        "osis:GetResourcePolicy",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "outposts:GetSite",
        "outposts:ListSites",
        "panorama:DescribeApplicationInstance",
        "panorama:DescribeApplicationInstanceDetails",
        "panorama:DescribePackage",
        "panorama:DescribePackageVersion",
        "panorama:ListApplicationInstances",
        "panorama:ListNodes",
        "panorama:ListPackages",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListServicePrincipalNames",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-ad:ListTemplateGroupAccessControlEntries",
        "pca-connector-ad:ListTemplates",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:ListChallengeMetadata",
        "pca-connector-scep:ListConnectors",
        "pca-connector-scep:ListTagsForResource",
```

```
        "pcs:GetCluster",
        "pcs:GetComputeNodeGroup",
        "pcs:GetQueue",
        "pcs:ListClusters",
        "pcs:ListComputeNodeGroups",
        "pcs:ListQueues",
        "pcs:ListTagsForResource",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "profile:GetDomain",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "qbusiness:GetApplication",
        "qbusiness:GetDataSource",
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetPolicy",
        "qbusiness:GetRetriever",
        "qbusiness:GetWebExperience",
        "qbusiness:ListApplications",
        "qbusiness:ListDataSources",
        "qbusiness:ListIndices",
        "qbusiness:ListPlugins",
        "qbusiness:ListRetrievers",
        "qbusiness:ListTagsForResource",
        "qbusiness:ListWebExperiences",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeCustomPermissions",
```

```
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeFolder",
        "quicksight:DescribeFolderPermissions",
        "quicksight:DescribeOAuthClientApplication",
        "quicksight:DescribeRefreshSchedule",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:DescribeTopic",
        "quicksight:DescribeVPCConnection",
        "quicksight:ListAnalyses",
        "quicksight:ListCustomPermissions",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListFolders",
        "quicksight:ListOAuthClientApplications",
        "quicksight:ListRefreshSchedules",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "quicksight:ListTopics",
        "quicksight:ListVPCConnections",
        "ram:GetPermission",
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares",
        "ram:ListPermissionAssociations",
        "ram:ListPermissions",
        "ram:ListPermissionVersions",
        "ram:ListResources",
        "ram:ListResourceSharePermissions",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
```

```
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBProxyTargetGroups",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeIntegrations",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterDbRevisions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeDataShares",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeIntegrations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeSnapshotCopyGrants",
        "redshift:DescribeTags",
        "redshift:GetResourcePolicy",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
```

```
        "refactor-spaces:GetRoute",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:DescribeCollection",
        "rekognition:DescribeProjects",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListCollections",
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "robomaker:DescribeRobotApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:ListRobotApplications",
        "robomaker:ListSimulationApplications",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53-recovery-control-config:DescribeCluster",
```

```
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:GetChange",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListCidrBlocks",
        "route53:ListCidrCollections",
        "route53:ListCidrLocations",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListQueryLoggingConfigs",
        "route53:ListResourceRecordSets",
        "route53:ListTagsForResource",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetOutpostResolver",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
```

```
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallDomains",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListOutpostResolvers",
        "route53resolver:ListResolverDnssecConfigs",
        "route53resolver:ListResolverEndpointIpAddresses",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRuleAssociations",
        "route53resolver:ListResolverRules",
        "route53resolver:ListTagsForResource",
        "rtbfabric:GetCertificateAssociation",
        "rtbfabric:GetInboundExternalLink",
        "rtbfabric:GetLink",
        "rtbfabric:GetLinkRoutingRule",
        "rtbfabric:GetOutboundExternalLink",
        "rtbfabric:GetRequesterGateway",
        "rtbfabric:GetResponderGateway",
        "rtbfabric:ListCertificateAssociations",
        "rtbfabric:ListLinkRoutingRules",
        "rtbfabric:ListLinks",
        "rtbfabric:ListRequesterGateways",
        "rtbfabric:ListResponderGateways",
        "rtbfabric:ListTagsForResource",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:ListTagsForResource",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListRegionalBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
```

```
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsInstances",
        "s3:ListAccessGrantsLocations",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
```

```
        "s3:ListTagsForResource",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
        "s3express:GetAccessPointScope",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:GetMetricsConfiguration",
        "s3express:ListAccessPointsForDirectoryBuckets",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:ListTagsForResource",
        "s3files:GetAccessPoint",
        "s3files:GetFileSystem",
        "s3files:GetFileSystemPolicy",
        "s3files:GetMountTarget",
        "s3files:GetSynchronizationConfiguration",
        "s3files:ListAccessPoints",
        "s3files:ListFileSystems",
        "s3files:ListMountTargets",
        "s3files:ListTagsForResource",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketMetricsConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableBucketReplication",
        "s3tables:GetTableBucketStorageClass",
        "s3tables:ListTableBuckets",
        "s3tables:ListTagsForResource",
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:ListIndexes",
        "s3vectors:ListTagsForResource",
        "s3vectors:ListVectorBuckets",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeClusterSchedulerConfig",
```

```
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeComputeQuota",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHub",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeMlflowApp",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelCardExportJob",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribeOptimizationJob",
        "sagemaker:DescribePartnerApp",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeStudioLifecycleConfig",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTrainingPlan",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
```

```
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListClusters",
        "sagemaker:ListClusterSchedulerConfigs",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListComputeQuotas",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHubs",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImages",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListMlflowApps",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCardExportJobs",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelCardVersions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringSchedules",
```

```
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListOptimizationJobs",
        "sagemaker:ListPartnerApps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSpaces",
        "sagemaker:ListStudioLifecycleConfigs",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingPlans",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "sdb:GetAttributes",
        "sdb:ListDomains",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetTargetDomains",
        "securityagent:GetApplication",
        "securityagent:ListApplications",
        "securityagent:ListPentests",
        "securityagent:ListTagsForResource",
        "securityagent:ListTargetDomains",
        "securityhub:DescribeHub",
```

```
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeStandardsControls",
        "securityhub:GetAggregatorV2",
        "securityhub:GetAutomationRuleV2",
        "securityhub:GetConfigurationPolicy",
        "securityhub:GetConfigurationPolicyAssociation",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindingAggregator",
        "securityhub:ListAggregatorsV2",
        "securityhub:ListAutomationRulesV2",
        "securityhub:ListConfigurationPolicies",
        "securityhub:ListConfigurationPolicyAssociations",
        "securityhub:ListEnabledProductsForImport",
        "securityhub:ListFindingAggregators",
        "securityhub:ListTagsForResource",
        "securitylake:GetSubscriber",
        "securitylake:ListDataLakeExceptions",
        "securitylake:ListDataLakes",
        "securitylake:ListLogSources",
        "securitylake:ListSubscribers",
        "securitylake:ListTagsForResource",
        "serviceCatalog:DescribePortfolioShares",
        "servicecatalog:DescribeServiceAction",
        "servicecatalog:DescribeTagOption",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListApplications",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:ListServiceActions",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:ListTagOptions",
        "servicediscovery:GetInstance",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:ListInstances",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
        "ses:DescribeReceiptRuleSet",
        "ses:GetAddonInstance",
        "ses:GetAddonSubscription",
        "ses:GetAddressList",
```

```
        "ses:GetArchive",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailTemplate",
        "ses:GetIngressPoint",
        "ses:GetRelay",
        "ses:GetRuleSet",
        "ses:GetTemplate",
        "ses:GetTrafficPolicy",
        "ses:ListAddonInstances",
        "ses:ListAddonSubscriptions",
        "ses:ListAddressLists",
        "ses:ListArchives",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListDedicatedIpPools",
        "ses:ListEmailTemplates",
        "ses:ListIngressPoints",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListRelays",
        "ses:ListRuleSets",
        "ses:ListTagsForResource",
        "ses:ListTemplates",
        "ses:ListTrafficPolicies",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeProtectionGroup",
        "shield:DescribeSubscription",
        "shield:ListProtectionGroups",
        "shield:ListTagsForResource",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningProfiles",
        "sms-voice:DescribeConfigurationSets",
        "sms-voice:DescribeKeywords",
        "sms-voice:DescribeOptOutLists",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeProtectConfigurations",
        "sms-voice:DescribeSenderIds",
```

```
        "sms-voice:GetProtectConfigurationCountryRuleSet",
        "sms-voice:GetResourcePolicy",
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "sns:GetDataProtectionPolicy",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:GetRotation",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListRotations",
        "ssm-contacts:ListTagsForResource",
        "ssm-guiconnect:GetConnectionRecordingPreferences",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-sap:ListTagsForResource",
        "ssm:DescribeAssociation",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeParameters",
        "ssm:DescribePatchBaselines",
        "ssm:GetAutomationExecution",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetMaintenanceWindow",
        "ssm:GetPatchBaseline",
```

```
        "ssm:GetResourcePolicies",
        "ssm:GetServiceSetting",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "sso:DescribeApplication",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetPermissionsBoundaryForPermissionSet",
        "sso:ListApplications",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
        "states:DescribeStateMachineAlias",
        "states:ListActivities",
        "states:ListStateMachineAliases",
        "states:ListStateMachines",
        "states:ListStateMachineVersions",
        "states:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:ListTagsForResource",
        "storagegateway:ListVolumes",
        "sts:GetCallerIdentity",
        "support:DescribeCases",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "textract:GetAdapter",
        "textract:ListAdapters",
        "textract:ListTagsForResource",
        "timestream-influxdb:GetDbCluster",
```

```
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:ListTagsForResource",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transcribe:GetCallAnalyticsJob",
        "transcribe:GetVocabularyFilter",
        "transcribe:ListCallAnalyticsJobs",
        "transcribe:ListTagsForResource",
        "transcribe:ListVocabularyFilters",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWebApp",
        "transfer:DescribeWebAppCustomization",
        "transfer:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListTagsForResource",
        "transfer:ListUsers",
        "transfer:ListWebApps",
        "transfer:ListWorkflows",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "verifiedpermissions:ListTagsForResource",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "vpc-lattice:GetAccessLogSubscription",
```

```
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourceConfiguration",
        "vpc-lattice:GetResourceGateway",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkResourceAssociation",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListResourceConfigurations",
        "vpc-lattice:ListResourceGateways",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworkResourceAssociations",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:GetWebACL",
        "waf-regional:GetWebACLForResource",
        "waf-regional:ListLoggingConfigurations",
        "waf:GetLoggingConfiguration",
        "waf:GetWebACL",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRuleGroup",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "wisdom:GetAIAgent",
        "wisdom:GetAIGuardrail",
        "wisdom:GetAIPrompt",
        "wisdom:GetAssistant",
        "wisdom:ListAIAgentVersions",
        "wisdom:ListAIGuardrails",
        "wisdom:ListAIGuardrailVersions",
        "wisdom:ListAIPromptVersions",
        "wisdom:ListAssistants",
        "workspaces-web:GetNetworkSettings",
```

```
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIpAccessSettings",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListUserSettings",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetIndexingRules",
        "xray:GetSamplingRules",
        "xray:GetTraceSegmentDestination",
        "xray:ListResourcePolicies",
        "xray:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConfigLogStreamStatementID",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*"
    },
    {
      "Sid" : "ConfigLogEventsStatementID",
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAccountActivityAccess

Deskripsi: Memungkinkan pengguna mengakses halaman Aktivitas Akun.

`AWSAccountActivityAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAccountActivityAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 20 Februari 2026, 20:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountActivityAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "payments:ListPaymentPreferences"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAccountManagementFullAccess

Deskripsi: Menyediakan akses penuh ke Manajemen AWS Akun.

`AWSAccountManagementFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAccountManagementFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 September 2021, 23:20 UTC
- Waktu teredit: 30 September 2021, 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "account:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAccountManagementReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke Manajemen Akun AWS

`AWSAccountManagementReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAccountManagementReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 September 2021, 23:29 UTC
- Waktu teredit: 30 September 2021, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:Get*",
        "account:List*"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAccountSettingsManagementRole

Deskripsi: Menyediakan izin yang diperlukan untuk mengelola akun untuk AWS aplikasi.

`AWSAccountSettingsManagementRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAccountSettingsManagementRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Desember 2025, 17:49 UTC
- Waktu teredit: 30 September 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountSettingsManagementRole`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetContactInformation",
        "account:PutContactInformation",
        "account:GetAccountInformation",
        "account:CloseAccount",
        "account:SendPhoneNumberVerification",
        "account:VerifyPhoneNumber"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "payments:ListTagsForResource",
        "payments:UntagResource",
        "payments:TagResource",
        "payments:ListPaymentPreferences",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:MakePayment",
        "payments:UpdatePaymentPreferences",
        "payments:CreatePaymentInstrument",
        "payments:UpdatePaymentInstrument",
        "payments:DeletePaymentInstrument",
        "payments:ListPaymentInstruments"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "invoicing:GetInvoicePDF"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "billing:GetSellerOfRecord"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "freetier:GetAccountPlanState"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ce:GetCostAndUsage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tax:GetTaxRegistration",
        "tax:PutTaxRegistration",
        "tax:ListTaxRegistrations",
        "tax:DeleteTaxRegistration",
        "tax:BatchPutTaxRegistration",
        "tax:GetTaxRegistrationDocument"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "customer-verification:GetCustomerVerificationDetails",
        "customer-verification:GetCustomerVerificationEligibility",
```

```
        "customer-verification:CreateCustomerVerificationDetails",
        "customer-verification:CreateUploadUrls",
        "customer-verification:UpdateCustomerVerificationDetails"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "sso:ListApplications",
        "sso:DescribeApplication",
        "sso:DescribeInstance"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeCases",
        "support:AddCommunicationToCase",
        "support:ResolveCase",
        "support:AddAttachmentsToSet",
        "support:DescribeAttachment",
        "support:DescribeCommunications"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAccountUsageReportAccess

Deskripsi: Memungkinkan pengguna mengakses halaman Laporan Penggunaan Akun.

`AWSAccountUsageReportAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAccountUsageReportAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 06 Februari 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountUsageReportAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewUsage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAgentlessDiscoveryService

Deskripsi: Menyediakan akses bagi Konektor Tanpa Agen Discovery untuk mendaftar dengan Layanan Penemuan AWS Aplikasi.

`AWSAgentlessDiscoveryService`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAgentlessDiscoveryService` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Agustus 2016, 01:35 UTC
- Waktu teredit: 24 Februari 2020, 23:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "awsconnector:RegisterConnector",
        "awsconnector:GetConnectorHealth"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::connector-platform-upgrade-info/*",
        "arn:aws:s3:::connector-platform-upgrade-info",
        "arn:aws:s3:::connector-platform-upgrade-bundles/*",
        "arn:aws:s3:::connector-platform-upgrade-bundles",
        "arn:aws:s3:::connector-platform-release-notes/*",
        "arn:aws:s3:::connector-platform-release-notes",
        "arn:aws:s3:::prod.agentless.discovery.connector.upgrade/*",
        "arn:aws:s3:::prod.agentless.discovery.connector.upgrade"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::import-to-ec2-connector-debug-logs/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "SNS:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
    },
    {
      "Sid" : "Discovery",
      "Effect" : "Allow",
      "Action" : [
        "Discovery:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "arsenal",
      "Effect" : "Allow",
      "Action" : [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAgentRegistryServiceRolePolicy

Deskripsi: Men AWS gizinkan Agen Registry mengakses sumber daya AWS layanan atas nama Anda

`AWSAgentRegistryServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 06 Agustus 2026, 14:27 UTC
- Waktu teredit: 21 Agustus 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAgentRegistryServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOrganizationsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowSLRCreationForAWSConfig",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowConfigRecorderWrite",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:PutServiceLinkedConfigurationRecorder"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "config:ConfigurationRecorderServicePrincipal" : [
            "agent-registry.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowConfigRecorderRead",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : [
        "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForAgentRegistry*"
      ]
    },
    {
```

```
      "Sid" : "AllowRegistryRecordReadWrite",
      "Effect" : "Allow",
      "Action" : [
        "agent-registry:CreateRegistryRecord",
        "agent-registry:DeleteRegistryRecord",
        "agent-registry:GetRegistryRecord",
        "agent-registry:ListRegistryRecords",
        "agent-registry:UpdateRegistryRecord"
      ],
      "Resource" : [
        "arn:aws:agent-registry:*:*:registry/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowPublishCloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/AgentRegistry",
            "AWS/Usage"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAppConfigServiceRolePolicy

Deskripsi: Memungkinkan AWS AppConfig untuk menelepon AWS layanan atas nama Anda.

`AWSAppConfigServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 08 Mei 2026, 18:42 UTC
- Waktu teredit: 08 Mei 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppConfigServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchPutExperimentMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AppConfig"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAppFabricFullAccess

Deskripsi: Menyediakan akses penuh ke AWS AppFabric layanan dan akses baca saja ke layanan dependen seperti S3, Kinesis, KMS.

`AWSAppFabricFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppFabricFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2023, 19:51 UTC
- Waktu teredit: 27 Juni 2023, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appfabric:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSListAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FirehoseReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowUseOfServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "appfabric.amazonaws.com"
        }
      },
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appfabric.amazonaws.com/
AWSServiceRoleForAppFabric"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAppFabricReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke AWS AppFabric

`AWSAppFabricReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppFabricReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2023, 19:52 UTC
- Waktu teredit: 27 Juni 2023, 19:52 UTC

- ARN: `arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appfabric:GetAppAuthorization",
        "appfabric:GetAppBundle",
        "appfabric:GetIngestion",
        "appfabric:GetIngestionDestination",
        "appfabric:ListAppAuthorizations",
        "appfabric:ListAppBundles",
        "appfabric:ListIngestionDestinations",
        "appfabric:ListIngestions",
        "appfabric:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAppFabricServiceRolePolicy

Deskripsi: Menye AppFabric diakan akses ke AWS sumber daya atas nama Anda

`AWSAppFabricServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 26 Juni 2023, 21:07 UTC
- Waktu teredit: 26 Juni 2023, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppFabricServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEmitMetric",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AppFabric"
        }
      }
    },
    {
      "Sid" : "S3PutObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*/AWSAppFabric/*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "FirehosePutRecord",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/AWSAppFabricManaged" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationAutoscalingAppStreamFleetPolicy

Deskripsi: Kebijakan yang memberikan izin ke Penskalaan Otomatis Aplikasi untuk mengakses AppStream dan CloudWatch.

`AWSApplicationAutoscalingAppStreamFleetPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 20 Oktober 2017, 19:04 UTC
- Waktu teredit: 20 Oktober 2017, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
```

```
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationAutoscalingCassandraTablePolicy

Deskripsi: Kebijakan pemberian izin ke Penskalaan Otomatis Aplikasi untuk mengakses Cassandra dan CloudWatch.

`AWSApplicationAutoscalingCassandraTablePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 18 Maret 2020, 22:49 UTC
- Waktu teredit: 18 Maret 2020, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cassandra:Select",
      "Resource" : [
        "arn:*:cassandra:*:*:/keyspace/system/table/*",
        "arn:*:cassandra:*:*:/keyspace/system_schema/table/*",
        "arn:*:cassandra:*:*:/keyspace/system_schema_mcs/table/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Alter",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationAutoscalingComprehendEndpointPolicy

Deskripsi: Kebijakan yang memberikan izin ke Penskalaan Otomatis Aplikasi untuk mengakses Memahami dan CloudWatch.

`AWSApplicationAutoscalingComprehendEndpointPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 14 November 2019, 18:39 UTC
- Waktu teredit: 14 November 2019, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingComprehendEndpointPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
```

```
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationAutoScalingCustomResourcePolicy

Deskripsi: Kebijakan pemberian izin ke Penskalaan Otomatis Aplikasi untuk mengakses ApigateWay dan CloudWatch untuk penskalaan sumber daya khusus

`AWSApplicationAutoScalingCustomResourcePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 04 Juni 2018, 23:22 UTC
- Waktu teredit: 04 Juni 2018, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationAutoscalingDynamoDBTablePolicy

Deskripsi: Kebijakan pemberian izin ke Penskalaan Otomatis Aplikasi untuk mengakses DynamoDB dan. CloudWatch

`AWSApplicationAutoscalingDynamoDBTablePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran

- Waktu pembuatan: 20 Oktober 2017, 21:34 UTC
- Waktu teredit: 20 Oktober 2017, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

Deskripsi: Kebijakan pemberian izin ke Penskalaan Otomatis Aplikasi untuk mengakses Armada Spot EC2 dan CloudWatch.

`AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 25 Oktober 2017, 18:23 UTC
- Waktu teredit: 25 Oktober 2017, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationAutoscalingECSServicePolicy

Deskripsi: Kebijakan pemberian izin ke Penskalaan Otomatis Aplikasi untuk mengakses Layanan Kontainer EC2 dan CloudWatch.

`AWSApplicationAutoscalingECSServicePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 25 Oktober 2017, 23:53 UTC
- Waktu yang diedit: 20 Mei 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:DescribeServiceRevisions",
        "ecs:UpdateService",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationAutoscalingElastiCacheRGPolicy

Deskripsi: Kebijakan pemberian izin ke Penskalaan Otomatis Aplikasi untuk mengakses Amazon ElastiCache dan Amazon CloudWatch.

`AWSApplicationAutoscalingElastiCacheRGPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 17 Agustus 2021, 23:41 UTC
- Waktu teredit: 26 Maret 2025, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingElastiCacheRGPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheActionsOnAllClusters",
      "Effect" : "Allow",
      "Action" : [
        "elasticache:DescribeReplicationGroups",
        "elasticache:ModifyCacheCluster",
        "elasticache:ModifyReplicationGroupShardConfiguration",
        "elasticache:IncreaseReplicaCount",
        "elasticache:DecreaseReplicaCount",
        "elasticache:DescribeCacheClusters",
```

```
        "elasticache:DescribeCacheParameters"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudWatchActionsOnAllAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ]
    },
    {
      "Sid" : "CloudWatchActionsOnTargetTrackingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationAutoscalingEMRInstanceGroupPolicy

Deskripsi: Kebijakan pemberian izin ke Penskalaan Otomatis Aplikasi untuk mengakses Elastic Map Reduce dan CloudWatch.

`AWSApplicationAutoscalingEMRInstanceGroupPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 26 Oktober 2017, 00:57 UTC
- Waktu teredit: 26 Oktober 2017, 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationAutoscalingKafkaClusterPolicy

Deskripsi: Kebijakan pemberian izin ke Penskalaan Otomatis Aplikasi untuk mengakses Streaming Terkelola untuk Apache Kafka dan CloudWatch.

`AWSApplicationAutoscalingKafkaClusterPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 24 Agustus 2020, 18:36 UTC
- Waktu teredit: 24 Agustus 2020 18.36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationAutoscalingLambdaConcurrencyPolicy

Deskripsi: Kebijakan pemberian izin ke Penskalaan Otomatis Aplikasi untuk mengakses Lambda dan CloudWatch.

`AWSApplicationAutoscalingLambdaConcurrencyPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran

- Waktu pembuatan: 21 Oktober 2019, 20:04 UTC
- Waktu teredit: 21 Oktober 2019, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:DeleteProvisionedConcurrencyConfig",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationAutoscalingNeptuneClusterPolicy

Deskripsi: Kebijakan pemberian izin ke Penskalaan Otomatis Aplikasi untuk mengakses Amazon Neptune dan Amazon CloudWatch.

`AWSApplicationAutoscalingNeptuneClusterPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 02 September 2021, 21:14 UTC
- Waktu teredit: 02 September 2021, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingNeptuneClusterPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterParameters",
```

```
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "rds:AddTagsToResource",
      "Resource" : [
        "arn:aws:rds:*:*:db:autoscaled-reader*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : "neptune"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "rds:CreateDBInstance",
      "Resource" : [
        "arn:aws:rds:*:*:db:autoscaled-reader*",
        "arn:aws:rds:*:*:cluster:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : "neptune"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:autoscaled-reader*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
```

```
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationAutoscalingRDSClusterPolicy

Deskripsi: Kebijakan pemberian izin ke Penskalaan Otomatis Aplikasi untuk mengakses RDS dan CloudWatch.

`AWSApplicationAutoscalingRDSClusterPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 17 Oktober 2017, 17:46 UTC
- Waktu teredit: 07 Agustus 2018, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CreateDBInstance",
        "rds:DeleteDBInstance",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "rds:ModifyDBCluster",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "rds.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationAutoscalingSageMakerEndpointPolicy

Deskripsi: Kebijakan yang memberikan izin ke Penskalaan Otomatis Aplikasi untuk mengakses SageMaker dan CloudWatch.

`AWSApplicationAutoscalingSageMakerEndpointPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 06 Februari 2018, 19:58 UTC
- Waktu teredit: 13 November 2023, 18:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "SageMaker",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateInferenceComponentRuntimeConfig",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SageMakerCloudWatchUpdate",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationAutoscalingWorkSpacesPoolPolicy

Deskripsi: Kebijakan pemberian izin ke Penskalaan Otomatis Aplikasi untuk mengakses Amazon WorkSpaces dan Amazon CloudWatch.

`AWSApplicationAutoscalingWorkSpacesPoolPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 17 Juni 2024, 18:39 UTC
- Waktu teredit: 17 Juni 2024, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingWorkSpacesPoolPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkSpacesActionsOnAllPools",
      "Effect" : "Allow",
      "Action" : [
        "workspaces:DescribeWorkspacesPools",
        "workspaces:UpdateWorkspacesPool"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchActionsOnAllAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchActionsOnTargetTrackingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationDiscoveryAgentAccess

Deskripsi: Menyediakan akses bagi Agen Penemuan untuk mendaftar dengan Layanan Penemuan AWS Aplikasi.

`AWSApplicationDiscoveryAgentAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationDiscoveryAgentAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Mei 2016, 21:38 UTC
- Waktu teredit: 24 Februari 2020, 22:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationDiscoveryAgentlessCollectorAccess

Deskripsi: Mengizinkan Pengumpul Tanpa Agen Layanan Penemuan Aplikasi untuk memperbarui, mendaftar, dan berkomunikasi secara otomatis dengan Layanan Penemuan Aplikasi

`AWSApplicationDiscoveryAgentlessCollectorAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationDiscoveryAgentlessCollectorAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 Agustus 2022, 21:00 UTC
- Waktu teredit: 16 Agustus 2022, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentlessCollectorAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:DescribeImages"
      ],
      "Resource" : "arn:aws:ecr-
public::446372222237:repository/6e5498e4-8c31-4f57-9991-13b4b992ff7b"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "sts:GetServiceBearerToken"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationDiscoveryServiceFullAccess

Deskripsi: Menyediakan akses penuh untuk melihat dan menandai Item Konfigurasi yang dikelola oleh Layanan Penemuan AWS Aplikasi

`AWSApplicationDiscoveryServiceFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationDiscoveryServiceFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Mei 2016, 21:30 UTC
- Waktu teredit: 19 Juni 2019, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryServiceFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:*",
        "discovery:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "continuousexport.discovery.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "migrationhub.amazonaws.com",
            "dmsintegration.migrationhub.amazonaws.com",
            "smsintegration.migrationhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationMigrationAgentInstallationPolicy

Deskripsi: Kebijakan ini memungkinkan penginstalan Agen AWS Replikasi, yang digunakan dengan Layanan Migrasi AWS Aplikasi (MGN) untuk memigrasikan server eksternal ke AWS. Lampirkan kebijakan ini ke pengguna atau peran IAM yang kredensialnya Anda berikan saat menginstal Agen AWS Replikasi.

`AWSApplicationMigrationAgentInstallationPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationAgentInstallationPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Juni 2022, 07:51 UTC
- Waktu teredit: 20 September 2022, 11:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentInstallationPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetAgentInstallationAssetsForMgn",
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:RegisterAgentForMgn",
        "mgn:VerifyClientRoleForMgn"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "mgn:IssueClientCertificateForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "mgn:TagResource",
      "Resource" : "arn:aws:mgn:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "mgn:CreateAction" : "RegisterAgentForMgn"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationMigrationAgentPolicy

Deskripsi: Kebijakan ini memungkinkan penginstalan dan penggunaan Agen AWS Replikasi, yang digunakan dengan Layanan Migrasi AWS Aplikasi (MGN) untuk memigrasikan server eksternal ke AWS. Lampirkan kebijakan ini ke pengguna atau peran IAM yang kredensialnya Anda berikan saat menginstal Agen AWS Replikasi.

`AWSApplicationMigrationAgentPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationAgentPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 April 2021, 07:00 UTC
- Waktu teredit: 20 September 2022, 11:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:RegisterAgentForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentInstallationAssetsForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
```

```
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "mgn:TagResource",
      "Resource" : "arn:aws:mgn:*:*:source-server/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationMigrationAgentPolicy_v2

Deskripsi: Kebijakan ini memungkinkan penggunaan Agen AWS Replikasi, yang digunakan dengan Layanan Migrasi AWS Aplikasi (MGN) untuk memigrasikan server eksternal ke AWS. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSApplicationMigrationAgentPolicy_v2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationAgentPolicy_v2` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Juni 2022, 14:14 UTC

- Waktu teredit: 06 Juni 2022 14:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn",
        "mgn:IssueClientCertificateForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/${aws:SourceIdentity}"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationMigrationConversionServerPolicy

Deskripsi: Kebijakan ini memungkinkan Server Konversi Layanan Migrasi Aplikasi (MGN), yang merupakan instans EC2 yang diluncurkan oleh Layanan Migrasi Aplikasi, untuk berkomunikasi dengan layanan MGN. Peran IAM dengan kebijakan ini dilampirkan (sebagai Profil Instans EC2) oleh MGN ke Server Konversi MGN, yang secara otomatis diluncurkan dan dihentikan oleh MGN, bila diperlukan. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda. Server Konversi MGN digunakan oleh Layanan Migrasi Aplikasi ketika pengguna memilih untuk meluncurkan instans Test atau Cutover menggunakan konsol MGN, CLI, atau API.

`AWSApplicationMigrationConversionServerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationConversionServerPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 April 2021, 06:48 UTC
- Waktu teredit: 07 April 2021, 06:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationConversionServerPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationMigrationEC2Access

Deskripsi: Kebijakan ini menyediakan operasi Amazon EC2 yang diperlukan untuk menggunakan Layanan Migrasi Aplikasi (MGN) untuk meluncurkan server yang dimigrasi sebagai instans EC2. Lampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSApplicationMigrationEC2Access`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationEC2Access` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 April 2021, 07:05 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeImages",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
```

```
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
```

```
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
            "CreateLaunchTemplate"
          ]
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:ModifyVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationMigrationFSxProxyPolicy

Deskripsi: Memberikan izin untuk mengelola sistem file ONTAP

`AWSApplicationMigrationFSxProxyPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationFSxProxyPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 31 Mei 2026, 13:12 UTC
- Waktu teredit: 09 Agustus 2026, 12:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationFSxProxyPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FSxSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:GetSecretValue",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "FSxDescribe",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeVolumes",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FSxCreateVolume",
```

```
      "Effect" : "Allow",
      "Action" : "fsx:CreateVolume",
      "Resource" : "arn:aws:fsx:*:*:volume/*/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "FSxCreateVolumeSVM",
      "Effect" : "Allow",
      "Action" : "fsx:CreateVolume",
      "Resource" : "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
    },
    {
      "Sid" : "FSxTagging",
      "Effect" : "Allow",
      "Action" : [
        "fsx:TagResource",
        "fsx:UntagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "FSxUpdateAndDeleteVolume",
      "Effect" : "Allow",
      "Action" : [
        "fsx:UpdateVolume",
        "fsx:DeleteVolume"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "FSxCreateSnapshot",
      "Effect" : "Allow",
      "Action" : "fsx:CreateSnapshot",
      "Resource" : "arn:aws:fsx:*:*:snapshot/*/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "FSxCreateSnapshotVolume",
      "Effect" : "Allow",
      "Action" : "fsx:CreateSnapshot",
      "Resource" : "arn:aws:fsx:*:*:volume/*/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "FSxDeleteSnapshot",
      "Effect" : "Allow",
      "Action" : "fsx:DeleteSnapshot",
      "Resource" : "arn:aws:fsx:*:*:snapshot/*/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "FSxTagSnapshot",
      "Effect" : "Allow",
      "Action" : "fsx:TagResource",
      "Resource" : "arn:aws:fsx:*:*:snapshot/*/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationMigrationFSxProxyVPCPolicy

Deskripsi: Memberikan izin untuk mengelola PrivateLink antara Layanan Migrasi AWS Aplikasi dan sistem file FSx pelanggan

`AWSApplicationMigrationFSxProxyVPCPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationFSxProxyVPCPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 31 Mei 2026, 13:27 UTC
- Waktu yang diedit: 31 Mei 2026, 13:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationFSxProxyVPCPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowlistAllVPCsforSGCreation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "CreateServiceEndpointResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc-endpoint-service/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/file_system_id" : "false",
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "EC2AllowOperationsOnTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVpcEndpointServiceConfigurations"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc-endpoint-service/*"
      ],
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/file_system_id" : "false",
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:GetSecurityGroupsForVpc",
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "ec2:DescribeInternetGateways",
        "elasticloadbalancing:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModifyVpcEndpointOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpointServicePermissions",
        "ec2:AcceptVpcEndpointConnections"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint-service/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/file_system_id" : "false",
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "EC2AllowTaggingOnCreate",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc-endpoint-service/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVpcEndpointServiceConfiguration"
          ]
        }
      }
    },
    {
      "Sid" : "CreateFSxNLB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/MgnFSxProxy*NLB/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/MgnFSxProxy*/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/file_system_id" : "false",
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "FSxNLBAllowTaggingOnCreate",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:AddTags",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/MgnFSxProxy*NLB/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/MgnFSxProxy*TG/*",
        "arn:aws:elasticloadbalancing:*:*:listener/net/MgnFSxProxy*/*/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateLoadBalancer",
            "CreateTargetGroup",
            "CreateListener"
          ]
        }
      }
    },
    {
      "Sid" : "FSxNLBRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "RegisterFSxTargetGroup",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:RegisterTargets",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:targetgroup/MgnFSxProxy*/*"
    },
    {
      "Sid" : "ELBv2AllowModify",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:ModifyLoadBalancerAttributes",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/MgnFSxProxy*/*"
    },
    {
      "Sid" : "ELBv2AllowOperationsOnTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/MgnFSxProxy*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/net/MgnFSxProxy*/*/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/MgnFSxProxy*/*"
```

```
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/file_system_id" : "false",
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationMigrationFullAccess

Deskripsi: Kebijakan ini memberikan izin ke semua API publik Layanan Migrasi AWS Aplikasi (MGN), serta izin untuk membaca informasi kunci KMS. Lampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSApplicationMigrationFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 April 2021, 06:56 UTC
- Waktu teredit: 03 Agustus 2026, 10:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess`

Versi kebijakan

Versi kebijakan: v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "mgn:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeKeyPairs",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
```

```
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor3",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor4",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor5",
      "Effect" : "Allow",
      "Action" : "iam:ListInstanceProfiles",
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor6",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole",
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithDrsRole"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "VisualEditor7",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "VisualEditor9",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor10",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "VisualEditor11",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
        "arn:aws:ssm:*:*:document/AWSMigration-*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "VisualEditor12",
      "Effect" : "Allow",
      "Action" : [
        "drs:DisconnectSourceServer"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceConfiguredDR" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "VisualEditor13",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
    },
    {
      "Sid" : "VisualEditor14",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor15",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*"
    },
    {
      "Sid" : "VisualEditor16",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
        "arn:aws:ssm:*:*:document/AWSMigration-*"
      ]
    },
    {
      "Sid" : "VisualEditor17",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
```

```
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor18",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSMigration-*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWSMigration-*:$DEFAULT"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "mgn.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor19",
      "Effect" : "Allow",
      "Action" : "ssm:ListCommands",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor20",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeParameters"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "FSxReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowTagSVMWithMapKeys",
      "Effect" : "Allow",
      "Action" : [
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:storage-virtual-machine/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "map-migrated",
            "aws-apn-id"
          ]
        }
      }
    },
    {
      "Sid" : "FSxDescribeOperations",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeVolumes",
        "fsx:DescribeSnapshots"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "FSxCreateVolume",
      "Effect" : "Allow",
      "Action" : "fsx:CreateVolume",
      "Resource" : [
        "arn:aws:fsx:*:*:volume/*/*",
        "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "FSxDeleteVolumeAndTag",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteVolume",
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "FSxCreateSnapshot",
      "Effect" : "Allow",
      "Action" : "fsx:CreateSnapshot",
      "Resource" : [
        "arn:aws:fsx:*:*:snapshot/*/*",
        "arn:aws:fsx:*:*:volume/*/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationMigrationMGHAccess

Deskripsi: Kebijakan ini memungkinkan Layanan Migrasi AWS Aplikasi (MGN) mengirim meta-data tentang kemajuan server yang dimigrasi menggunakan MGN ke AWS Migrasi Hub (MGH). MGN secara otomatis membuat peran IAM dengan kebijakan ini terlampir, dan mengambil peran ini. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSApplicationMigrationMGHAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationMGHAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 April 2021, 07:10 UTC
- Waktu teredit: 07 April 2021, 07:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationMGHAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationMigrationNetworkMigrationCustomResource

Deskripsi: Memberikan izin untuk sumber daya kustom Migrasi Jaringan

`AWSApplicationMigrationNetworkMigrationCustomResource`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationNetworkMigrationCustomResource` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 November 2025, 11:34 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationNetworkMigrationCustomResource`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ModifyTGW",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyTransitGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationMigrationNetworkMigrationMultiAccount

Deskripsi: Memberikan izin untuk mengotomatiskan migrasi infrastruktur VMware ke AWS jaringan melalui CloudFormation

`AWSApplicationMigrationNetworkMigrationMultiAccount`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationNetworkMigrationMultiAccount` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 November 2025, 09:04 UTC
- Waktu teredit: 15 September 2026, 13:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationNetworkMigrationMultiAccount`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2CFNReadonlyPrefixList",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:prefix-list/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "NetworkAnalyzer",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreatePermissionsByCFNNACL",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceNetworkAclAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByCFNNACLSN",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceNetworkAclAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "EC2CFNReadonly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
```

```
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "MGNCFNDescribe",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*"
    },
    {
      "Sid" : "CFNCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
```

```
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CFNTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack",
            "UpdateStack"
          ]
        }
      }
    },
    {
      "Sid" : "CFNOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CFNProvision",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2PutResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2ResourceOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
```

```
      }
    },
    {
      "Sid" : "AnalyzerEC2ResourceSgTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2RequestSgTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2SecurityGroupTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "ec2:CreateAction" : [
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "EC2TagCFNSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByCFN",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateNatGateway",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayVpcAttachment",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInsightsPath"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:network-insights-path/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
```

```
      "Sid" : "AllowCreateTGWVpcAttachmentSameOrg",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        }
      }
    },
    {
      "Sid" : "CFNProvisionNetworking",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateVpc",
        "ec2:CreateTransitGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:transit-gateway/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagNetworking",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateNetworkAcl",
        "ec2:CreateSubnet",
        "ec2:CreateRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagRouting",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
```

```
    {
      "Sid" : "CreatePermissionsByRequestTagNAT",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNatGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagTransitGateway",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
```

```
    {
      "Sid" : "CreatePermissionsByRequestTagTGWAttachment",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "DeleteENI",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagInsights",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsPath"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-insights-path/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "EC2TagCFN",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-policy-table/*",
        "arn:aws:ec2:*:*:transit-gateway-connect-peer/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:subnet/*",
```

```
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:network-insights-path/*",
        "arn:aws:ec2:*:*:network-insights-access-scope-analysis/*",
        "arn:aws:ec2:*:*:network-insights-access-scope/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:network-insights-analysis/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "ec2:CreateAction" : [
            "CreateTransitGatewayVpcAttachment",
            "CreateTransitGatewayRouteTableAnnouncement",
            "CreateTransitGatewayRouteTable",
            "CreateTransitGatewayRoute",
            "CreateTransitGatewayPrefixListReference",
            "CreateTransitGatewayPolicyTable",
            "CreateTransitGatewayPeeringAttachment",
            "CreateTransitGatewayConnectPeer",
            "CreateTransitGatewayConnect",
            "CreateTransitGateway",
            "CreateInternetGateway",
            "CreateNatGateway",
            "CreateSubnet",
            "CreateNetworkAcl",
            "CreateRouteTable",
            "CreateNetworkInterface",
            "CreateNetworkInsightsPath",
            "CreateNetworkInsightsAccessScope",
            "CreateLaunchTemplate",
            "AllocateAddress",
            "StartNetworkInsightsAnalysis",
            "CreateVpc"
          ]
        }
      }
    },
    {
      "Sid" : "deployerWorkload",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/network-migration/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "putParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/network-migration/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "deleteParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter",
        "ssm:DeleteResourcePolicy",
        "ssm:ListTagsForResource"
      ],
```

```
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/network-migration/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "ramResourceSharing",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutResourcePolicy",
        "ssm:GetResourcePolicies"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/network-migration/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ramTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
```

```
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreateResourceShareTransitGateway",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "Bool" : {
          "ram:RequestedAllowsExternalPrincipals" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AssociateResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService",
          "ram:RequestedResourceType" : [
```

```
            "ec2:TransitGateway",
            "ssm:Parameter"
          ]
        }
      }
    },
    {
      "Sid" : "CreateResourceShareWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare",
        "ram:DisassociateResourceShare",
        "ram:UpdateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AllowGetResourceShares",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*"
    },
    {
      "Sid" : "CreateCustomResourceLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/network-migration-modify-tgw*"
```

```
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateCustomResourceLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:TagResource"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:network-migration*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "GetCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:ListTags"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:network-migration*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OperationsCustomResourceLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:DeleteFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:network-migration*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreateRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
```

```
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "PassGetRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OperationsRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
```

```
        "iam:GetRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AttachCustomResourceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole",
            "arn:aws:iam::aws:policy/
AWSApplicationMigrationNetworkMigrationCustomResource"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "MGNCFNBasedResourcesProvision",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:AcceptTransitGatewayVpcAttachment",
        "ec2:AssociateNatGatewayAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateTransitGatewayRouteTable",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteNetworkInsightsAnalysis",
        "ec2:DeleteNetworkInsightsPath",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeleteSubnet",
        "ec2:DeleteTransitGateway",
        "ec2:DeleteTransitGatewayRoute",
        "ec2:DeleteTransitGatewayRouteTable",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:DeleteVolume",
        "ec2:DeleteVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachVolume",
        "ec2:DisableTransitGatewayRouteTablePropagation",
        "ec2:DisassociateNatGatewayAddress",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyLaunchTemplate",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyTransitGateway",
        "ec2:ModifyTransitGatewayVpcAttachment",
        "ec2:ModifyVolume",
```

```
        "ec2:ModifyVpcAttribute",
        "ec2:RejectTransitGatewayVpcAttachment",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceTransitGatewayRoute",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAnalysis"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-policy-table/*",
        "arn:aws:ec2:*:*:transit-gateway-connect-peer/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:network-insights-path/*",
        "arn:aws:ec2:*:*:network-insights-access-scope-analysis/*",
        "arn:aws:ec2:*:*:network-insights-access-scope/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:network-insights-analysis/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
```

```
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreateTransitGatewaySLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/transitgateway.amazonaws.com/
AWSServiceRoleForVPCTransitGateway"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "transitgateway.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AnalyzerENIResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationMigrationReadOnlyAccess

Deskripsi: Kebijakan ini memberikan izin ke semua API publik read-only dari Application Migration Service (MGN), serta beberapa API read-only dari AWS layanan lain yang diperlukan untuk menggunakan konsol MGN secara penuh baca-saja. Lampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSApplicationMigrationReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 April 2021, 07:15 UTC
- Waktu teredit: 01 Juli 2026, 14:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "mgn:DescribeJobLogItems",
        "mgn:DescribeJobs",
        "mgn:DescribeSourceServers",
        "mgn:DescribeReplicationConfigurationTemplates",
        "mgn:GetLaunchConfiguration",
        "mgn:DescribeVcenterClients",
        "mgn:GetReplicationConfiguration",
        "mgn:DescribeLaunchConfigurationTemplates",
        "mgn:ListSourceServerActions",
        "mgn:ListTemplateActions",
        "mgn:ListApplications",
        "mgn:ListWaves",
        "mgn:ListExports",
        "mgn:ListImports",
        "mgn:ListImportErrors",
        "mgn:ListExportErrors"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationMigrationReplicationServerPolicy

Deskripsi: Kebijakan ini memungkinkan Server Replikasi Layanan Migrasi Aplikasi (MGN), yang merupakan instans EC2 yang diluncurkan oleh Layanan Migrasi Aplikasi - untuk berkomunikasi dengan layanan MGN, dan membuat snapshot EBS di layanan Anda. Akun AWS Peran IAM dengan kebijakan ini dilampirkan (sebagai Profil Instans EC2) oleh Layanan Migrasi Aplikasi ke Server Replikasi MGN yang secara otomatis diluncurkan dan dihentikan oleh MGN, sesuai kebutuhan. Server Replikasi MGN digunakan untuk memfasilitasi replikasi data dari server eksternal Anda ke AWS, sebagai bagian dari proses migrasi yang dikelola menggunakan MGN. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSApplicationMigrationReplicationServerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationReplicationServerPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 April 2021, 07:21 UTC
- Waktu teredit: 31 Mei 2026, 13:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationReplicationServerPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn",
        "mgn:GetAgentSnapshotCreditsForMgn",
        "mgn:DescribeReplicationServerAssociationsForMgn",
        "mgn:DescribeSnapshotRequestsForMgn",
        "mgn:BatchDeleteSnapshotRequestForMgn",
        "mgn:NotifyAgentAuthenticationForMgn",
        "mgn:BatchCreateVolumeSnapshotGroupForMgn",
        "mgn:UpdateAgentReplicationProcessStateForMgn",
        "mgn:NotifyAgentReplicationProgressForMgn",
        "mgn:NotifyAgentConnectedForMgn",
        "mgn:NotifyAgentDisconnectedForMgn",
        "mgn:StartSnapshotGroupForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationMigrationServiceEc2InstancePolicy

Deskripsi: Kebijakan ini memungkinkan menginstal dan menggunakan Agen AWS Replikasi, yang digunakan oleh Layanan Migrasi AWS Aplikasi (AWS MGN) untuk memigrasikan server sumber yang berjalan di EC2 (Lintas wilayah atau lintas AZ). Peran IAM dengan kebijakan ini harus dilampirkan (sebagai Profil Instans EC2) ke Instans EC2.

`AWSApplicationMigrationServiceEc2InstancePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationServiceEc2InstancePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 Agustus 2023, 13:19 UTC
- Waktu teredit: 03 Januari 2024, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationServiceEc2InstancePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MgnAgentInstallation",
```

```
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientLogsForMgn",
        "mgn:RegisterAgentForMgn",
        "mgn:GetAgentInstallationAssetsForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MgnAgentReplication",
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/*"
    },
    {
      "Sid" : "MgnSourceServerTagResource",
      "Effect" : "Allow",
      "Action" : "mgn:TagResource",
      "Resource" : "arn:aws:mgn:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "mgn:CreateAction" : "RegisterAgentForMgn"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationMigrationServiceRolePolicy

Deskripsi: Men AWS gizinkan Layanan Migrasi aplikasi untuk membuat dan mengelola AWS sumber daya atas nama Anda.

`AWSApplicationMigrationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 07 April 2021, 06:43 UTC
- Waktu teredit: 19 Juli 2026, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationMigrationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : "mgn:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : "arn:aws:organizations::*:account/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage",
        "ec2:DeregisterImage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
```

```
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
```

```
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationReplicationServerRole",
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
            "RegisterImage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
```

```
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationMigrationSSMAccess

Deskripsi: Kebijakan ini menyediakan akses ke operasi Amazon SSM yang diperlukan untuk menggunakan Layanan Migrasi Aplikasi (MGN) untuk menjalankan dokumen SSM perintah pasca migrasi kustom. Lampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSApplicationMigrationSSMAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationSSMAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2022, 09:29 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/*:*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocumentVersions",
        "ssm:GetDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSApplicationMigrationVCenterClientPolicy

Deskripsi: Kebijakan ini memungkinkan penginstalan dan penggunaan AWS vCenter Client, yang digunakan dengan Layanan Migrasi AWS Aplikasi (MGN) untuk memigrasikan server eksternal ke. AWS Lampirkan kebijakan ini ke pengguna atau peran IAM yang kredensialnya Anda berikan saat menginstal Klien AWS vCenter.

`AWSApplicationMigrationVCenterClientPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationVCenterClientPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 November 2021, 12:53 UTC
- Waktu teredit: 08 November 2021, 12:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:CreateVcenterClientForMgn",
        "mgn:DescribeVcenterClients"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetVcenterClientCommandsForMgn",
        "mgn:SendVcenterClientCommandResultForMgn",
        "mgn:SendVcenterClientLogsForMgn",
        "mgn:SendVcenterClientMetricsForMgn",
        "mgn:DeleteVcenterClient",
        "mgn:TagResource",
        "mgn:NotifyVcenterClientStartedForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:vcenter-client/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAppMeshEnvoyAccess

Deskripsi: Kebijakan App Mesh Envoy untuk mengakses konfigurasi Node Virtual.

`AWSAppMeshEnvoyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppMeshEnvoyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Juli 2019, 21:29 UTC
- Waktu teredit: 03 Juli 2019, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh:StreamAggregatedResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAppMeshFullAccess

Deskripsi: Menyediakan akses penuh ke API AWS App Mesh dan Konsol Manajemen.

`AWSAppMeshFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppMeshFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 April 2019, 17:50 UTC
- Waktu teredit: 07 Januari 2021 19.54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appmesh.amazonaws.com/
AWSServiceRoleForAppMesh",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "appmesh.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStack*",
        "cloudformation:UpdateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSAppMesh-GettingStarted-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "acm:DescribeCertificate",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAppMeshPreviewEnvoyAccess

Deskripsi: Kebijakan Utusan Pratinjau App Mesh untuk mengakses konfigurasi Node Virtual.

`AWSAppMeshPreviewEnvoyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppMeshPreviewEnvoyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Agustus 2019, 23:32 UTC
- Waktu teredit: 05 Agustus 2019, 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh-preview:StreamAggregatedResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAppMeshPreviewServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh AWS App Mesh

`AWSAppMeshPreviewServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 19 Juni 2019, 19:07 UTC
- Waktu teredit: 21 Agustus 2019, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAppMeshReadOnly

Deskripsi: Menyediakan akses baca-saja ke API AWS App Mesh dan Konsol Manajemen.

`AWSAppMeshReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppMeshReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 April 2019, 17:51 UTC
- Waktu teredit: 07 Januari 2021 19.53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshReadOnly`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh:Describe*",
        "appmesh:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*"
      ],
```

```
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSAppMesh-GettingStarted-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "acm:DescribeCertificate",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAppMeshServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh AWS AppMesh

`AWSAppMeshServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 03 Juni 2019, 18:30 UTC
- Waktu teredit: 10 Oktober 2023, 16:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAppRunnerFullAccess

Deskripsi: Memberikan izin untuk semua tindakan App Runner.

`AWSAppRunnerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppRunnerFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Januari 2022, 04:02 UTC
- Waktu teredit: 11 Januari 2022, 04:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/apprunner.amazonaws.com/
AWSServiceRoleForAppRunner",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "apprunner.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "apprunner.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AppRunnerAdminAccess",
      "Effect" : "Allow",
      "Action" : "apprunner:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAppRunnerReadOnlyAccess

Deskripsi: Memberikan izin untuk membuat daftar dan melihat detail tentang sumber daya App Runner.

`AWSAppRunnerReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppRunnerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Februari 2022, 21:24 UTC
- Waktu teredit: 24 Februari 2022, 21:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apprunner:List*",
        "apprunner:Describe*"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAppRunnerServicePolicyForECRAccess

Deskripsi: Kebijakan layanan AWS App Runner yang memberikan izin baca ke sumber daya Amazon ECR di akun pelanggan. Gunakan dalam peran yang diteruskan ke App Runner saat membuat atau memperbarui layanan App Runner.

`AWSAppRunnerServicePolicyForECRAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppRunnerServicePolicyForECRAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Mei 2021, 19:17 UTC
- Waktu teredit: 14 Mei 2021 19.17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAppSyncAdministrator

Deskripsi: Menyediakan akses administratif ke AppSync layanan, meskipun tidak cukup untuk mengakses melalui konsol.

`AWSAppSyncAdministrator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppSyncAdministrator` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 Maret 2018, 21:20 UTC
- Waktu teredit: 04 November 2019, 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncAdministrator`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "appsync.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "appsync.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appsync.amazonaws.com/
AWSServiceRoleForAppSync*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAppSyncInvokeFullAccess

Deskripsi: Menyediakan akses panggilan penuh ke AppSync layanan - baik melalui konsol maupun secara independen

`AWSAppSyncInvokeFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppSyncInvokeFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 Maret 2018, 21:21 UTC
- Waktu teredit: 20 Maret 2018, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAppSyncPushToCloudWatchLogs

Deskripsi: AppSync Memungkinkan untuk mendorong log ke CloudWatch akun pengguna.

`AWSAppSyncPushToCloudWatchLogs`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppSyncPushToCloudWatchLogs` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 09 April 2018, 19:38 UTC
- Waktu teredit: 09 April 2018, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAppSyncSchemaAuthor

Deskripsi: Menyediakan akses untuk membuat, memperbarui, dan menanyakan skema.

`AWSAppSyncSchemaAuthor`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppSyncSchemaAuthor` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 Maret 2018, 21:21 UTC
- Waktu teredit: 01 Februari 2023, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:CreateResolver",
        "appsync:CreateType",
        "appsync:DeleteResolver",
        "appsync:DeleteType",
        "appsync:GetResolver",
        "appsync:GetType",
        "appsync:GetDataSource",
        "appsync:GetSchemaCreationStatus",
        "appsync:GetIntrospectionSchema",
        "appsync:GetGraphqlApi",
        "appsync:ListTypes",
        "appsync:ListApiKeys",
        "appsync:ListResolvers",
        "appsync:ListDataSources",
        "appsync:ListGraphqlApis",
        "appsync:StartSchemaCreation",
        "appsync:UpdateResolver",
        "appsync:UpdateType",
        "appsync:TagResource",
        "appsync:UntagResource",
        "appsync:ListTagsForResource",
        "appsync:CreateFunction",
        "appsync:UpdateFunction",
        "appsync:GetFunction",
        "appsync:DeleteFunction",
        "appsync:ListFunctions",
        "appsync:ListResolversByFunction",
        "appsync:EvaluateMappingTemplate",
        "appsync:EvaluateCode"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAppSyncServiceRolePolicy

Deskripsi: Mengaktifkan akses ke AWS layanan dan sumber daya yang digunakan atau dikelola oleh AppSync

`AWSAppSyncServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 21 Januari 2020, 19:56 UTC
- Waktu teredit: 21 Januari 2020, 19:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSArtifactAccountSync

Deskripsi: Mengizinkan akses read-only AWS Artifact ke operasi di Organisasi. AWS

`AWSArtifactAccountSync`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSArtifactAccountSync` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 10 April 2018, 23:04 UTC
- Waktu teredit: 10 April 2018, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSArtifactAgreementsFullAccess

Deskripsi: Kebijakan ini memberikan izin penuh untuk membuat daftar, mengunduh, menerima, dan mengakhiri perjanjian AWS Artifact. Ini juga mencakup izin untuk membuat daftar dan mengaktifkan akses AWS layanan di layanan Organisasi, serta menjelaskan detail organisasi. Selain itu, kebijakan ini menyediakan kemampuan untuk memeriksa apakah peran terkait layanan yang diperlukan ada dan membuatnya jika tidak

`AWSArtifactAgreementsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSArtifactAgreementsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 November 2024, 19:36 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactAgreementsFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListAgreementActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSAgreementActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource" : "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid" : "CustomerAgreementActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource" : "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetRoleToCheckForRoleExistence",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Sid" : "EnableServiceTrust",
      "Effect" : "Allow",
```

```
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EnableServiceTrustForArtifact",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "aws-artifact-account-sync.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSArtifactAgreementsReadOnlyAccess

Deskripsi: Kebijakan ini memberikan akses baca-saja untuk mencantumkan perjanjian layanan AWS Artifact dan mengunduh perjanjian yang diterima.. Ini juga mencakup izin untuk daftar serta menjelaskan detail organisasi. Selain itu, kebijakan ini menyediakan kemampuan untuk memeriksa apakah peran terkait layanan yang diperlukan ada.

`AWSArtifactAgreementsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSArtifactAgreementsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 November 2024, 19:36 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactAgreementsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListAgreementsActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetCustomerAgreementActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetCustomerAgreement"
      ],
```

```
      "Resource" : "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid" : "AWSOrganizationActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSArtifactComplianceInquiriesFullAccess

Deskripsi: Menyediakan akses penuh ke Penyelidikan Kepatuhan Artefak.

`AWSArtifactComplianceInquiriesFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSArtifactComplianceInquiriesFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Juni 2026, 19:27 UTC
- Waktu teredit: 30 September 2026, 22:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactComplianceInquiriesFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListAndCreateComplianceInquiryActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:ListComplianceInquiries",
        "artifact:CreateComplianceInquiry"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ComplianceInquiryActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:ListComplianceInquiryQueries",
        "artifact:GetComplianceInquiryMetadata",
        "artifact:ExportComplianceInquiry",
        "artifact:PutComplianceInquiryFeedback"
      ],
      "Resource" : "arn:aws:artifact:*:*:compliance-inquiry/*"
    },
```

```
    {
      "Sid" : "NotificationConfigurationListActions",
      "Effect" : "Allow",
      "Action" : [
        "notifications:ListNotificationConfigurations",
        "notifications:ListChannels",
        "notifications:ListEventRules"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NotificationConfigurationContactReadActions",
      "Effect" : "Allow",
      "Action" : [
        "notifications-contacts:GetEmailContact"
      ],
      "Resource" : "arn:aws:notifications-contacts::*:emailcontact/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSArtifactComplianceInquiriesReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke Penyelidikan Kepatuhan Artefak.

`AWSArtifactComplianceInquiriesReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSArtifactComplianceInquiriesReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Juni 2026, 19:42 UTC
- Waktu teredit: 30 Juni 2026, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactComplianceInquiriesReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListComplianceInquiryActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:ListComplianceInquiries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetComplianceInquiryActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetComplianceInquiryMetadata",
        "artifact:ListComplianceInquiryQueries",
        "artifact:ExportComplianceInquiry"
      ],
      "Resource" : "arn:aws:artifact:*:*:compliance-inquiry/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSArtifactReportsReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke laporan layanan AWS Artifact.

`AWSArtifactReportsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSArtifactReportsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Januari 2024, 22:42 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports",
        "artifact:ListReportVersions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSArtifactServiceRolePolicy

Deskripsi: AWS Mengizinkan Artifact mengumpulkan informasi tentang organisasi melalui layanan AWS Organisasi.

`AWSArtifactServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 21 Agustus 2023, 20:27 UTC

- Waktu teredit: 21 Agustus 2023, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAuditManagerAdministratorAccess

Deskripsi: Menyediakan akses administratif untuk mengaktifkan atau menonaktifkan AWS Audit Manager, memperbarui pengaturan, dan mengelola penilaian, kontrol, dan kerangka kerja

`AWSAuditManagerAdministratorAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAuditManagerAdministratorAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Desember 2020, 20:02 UTC
- Waktu teredit: 15 Mei 2024, 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAuditManagerAdministratorAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AuditManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "auditmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccountsForParent",
```

```
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOnlyAuditManagerIntegration",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "auditmanager.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser",
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMAccessCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*",
      "Condition" : {
        "StringLike" : {
```

```
          "iam:AWSServiceName" : "auditmanager.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMAccessManageSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:UpdateRoleDescription",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*"
    },
    {
      "Sid" : "S3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsCreateGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
```

```
        "StringLike" : {
          "kms:ViaService" : "auditmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SNSAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported"
        },
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.securityhub"
          ]
        }
      }
    },
    {
      "Sid" : "EventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
```

```
    },
    {
      "Sid" : "TagAccess",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ControlCatalogAccess",
      "Effect" : "Allow",
      "Action" : [
        "controlcatalog:ListCommonControls",
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAuditManagerServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Manajer AWS Audit

`AWSAuditManagerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 08 Desember 2020, 15:12 UTC
- Waktu teredit: 02 Juni 2026, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:ListBackupPlans",
        "backup:ListRecoveryPointsByResource",
        "bedrock:GetCustomModel",
        "bedrock:GetFoundationModel",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListCustomModels",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListModelCustomizationJobs",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListDistributions",
```

```
        "cloudtrail:GetTrail",
        "cloudtrail:ListTrails",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cognito-idp:DescribeUserPool",
        "config:DescribeConfigRules",
        "config:DescribeDeliveryChannels",
        "config:ListDiscoveredResources",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTable",
        "dynamodb:ListBackups",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:GetLaunchTemplateData",
        "ec2:DescribeAddresses",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
```

```
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ecs:DescribeClusters",
        "eks:DescribeAddonVersions",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeServiceUpdates",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeSslPolicies",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListSecurityConfigurations",
        "events:DescribeRule",
        "events:ListConnections",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRules",
        "firehose:ListDeliveryStreams",
        "fsx:DescribeFileSystems",
        "guardduty:ListDetectors",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccessKeyLastUsed",
        "iam:GetCredentialReport",
        "iam:GetGroupPolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupsForUser",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListOpenIdConnectProviders",
```

```
        "iam:ListPolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSamlProviders",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "iam:ListPolicyVersions",
        "iam:ListAccessKeys",
        "iam:ListAttachedRolePolicies",
        "iam:ListMfaDeviceTags",
        "iam:ListMfaDevices",
        "kafka:ListClusters",
        "kafka:ListKafkaVersions",
        "kinesis:ListStreams",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListGrants",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "lambda:ListFunctions",
        "license-manager:ListAssociationsForLicenseConfiguration",
        "license-manager:ListLicenseConfigurations",
        "license-manager:ListUsageForLicenseConfiguration",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:DescribeResourcePolicies",
        "logs:FilterLogEvents",
        "logs:GetDataProtectionPolicy",
        "es:DescribeDomains",
        "es:DescribeDomain",
        "es:DescribeDomainConfig",
        "es:ListDomainNames",
        "organizations:DescribeOrganization",
        "organizations:DescribePolicy",
        "organizations:DescribeAccount",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
```

```
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeLoggingStatus",
        "route53:GetQueryLoggingConfig",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpoints",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListModels",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListUserProfiles",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketVersioning",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:ListAllMyBuckets",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecrets",
        "securityhub:DescribeStandards",
        "sns:ListTagsForResource",
        "sns:ListTopics",
```

```
        "sqs:ListQueues",
        "waf-regional:GetRule",
        "waf-regional:GetWebAcl",
        "waf:GetRule",
        "waf:GetRuleGroup",
        "waf:ListActivatedRulesInRuleGroup",
        "waf:ListWebAcls",
        "wafv2:ListWebAcls",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:ListRuleGroups",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListWebACLs",
        "waf-regional:ListRules",
        "waf:ListRuleGroups",
        "waf:ListRules"
      ],
      "Resource" : "*",
      "Sid" : "APIsAccess"
    },
    {
      "Sid" : "S3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:GetBucketLogging",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketTagging"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "APIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
```

```
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/restapis/*/stages"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "CreateEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported",
          "events:source" : [
            "aws.securityhub"
          ]
        },
        "Null" : {
          "events:source" : "false",
          "events:detail-type" : "false"
        }
      }
    },
    {
      "Sid" : "EventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
```

```
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSAutoScalingPlansEC2AutoScalingPolicy

Deskripsi: Kebijakan yang memberikan izin ke Penskalaan AWS Otomatis untuk meramalkan kapasitas secara berkala dan menghasilkan tindakan penskalaan terjadwal untuk grup Penskalaan Otomatis dalam rencana penskalaan

`AWSAutoScalingPlansEC2AutoScalingPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 23 Agustus 2018, 22:46 UTC
- Waktu teredit: 23 Agustus 2018, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBackupAccessPointOperatorAccess

Deskripsi: Kebijakan ini memberikan izin kepada pengguna untuk membuat dan mengelola titik akses cadangan untuk mengakses data cadangan di titik pemulihan melalui titik akses S3.

`AWSBackupAccessPointOperatorAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupAccessPointOperatorAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Agustus 2026, 16:12 UTC
- Waktu teredit: 06 Agustus 2026, 16:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupAccessPointOperatorAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateBackupAccessPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupAccessPoint"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*"
    },
    {
      "Sid" : "BackupAccessPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeBackupAccessPoint",
        "backup:DeleteBackupAccessPoint"
      ],
      "Resource" : "arn:aws:backup:*:*:accesspoint/*"
    },
    {
      "Sid" : "ListBackupAccessPointPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "backup:ListBackupAccessPoints",
        "backup:ListBackupAccessPointsByResource",
        "backup:ListBackupAccessPointsByRecoveryPoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3AccessPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateAccessPoint",
        "s3:DeleteAccessPoint",
        "s3:GetAccessPoint",
        "s3:PutAccessPointPolicy"
      ],
      "Resource" : "arn:aws:s3:*:*:accesspoint/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "backup.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DecryptKMSEncryptedDataByAWSBackup",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "backup.*.amazonaws.com",
          "kms:EncryptionContext:aws:backup:backup-vault" : "*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBackupAuditAccess

Deskripsi: Kebijakan ini memberikan izin bagi pengguna untuk membuat kontrol dan kerangka kerja yang menentukan harapan mereka untuk sumber daya dan aktivitas AWS Cadangan, serta untuk mengaudit AWS sumber daya dan aktivitas Cadangan terhadap kontrol dan kerangka kerja yang ditentukan. Kebijakan ini memberikan izin ke AWS Config dan layanan serupa untuk menjelaskan harapan pengguna melakukan audit. Kebijakan ini juga memberikan izin untuk mengirimkan laporan audit ke S3 dan layanan serupa, dan memungkinkan pengguna menemukan dan membuka laporan audit mereka.

`AWSBackupAuditAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupAuditAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Agustus 2021, 01:02 UTC
- Waktu teredit: 10 April 2023, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupAuditAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateFramework",
        "backup:UpdateFramework",
        "backup:ListFrameworks",
        "backup:DescribeFramework",
        "backup:DeleteFramework",
        "backup:ListBackupPlans",
        "backup:ListBackupVaults",
        "backup:CreateReportPlan",
        "backup:UpdateReportPlan",
        "backup:ListReportPlans",
        "backup:DescribeReportPlan",
        "backup:DeleteReportPlan",
        "backup:StartReportJob",
        "backup:ListReportJobs",
        "backup:DescribeReportJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeComplianceByConfigRule"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:GetComplianceDetailsByConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBackupDataTransferAccess

Deskripsi: Kebijakan ini memungkinkan agen AWS Backint menyelesaikan transfer data AWS cadangan dengan bidang Penyimpanan Cadangan. Lampirkan kebijakan ini ke peran yang diasumsikan oleh Instans EC2 yang menjalankan SAP HANA dengan agen Backint.

`AWSBackupDataTransferAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupDataTransferAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 November 2022, 22:48 UTC
- Waktu teredit: 10 November 2022, 22.48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupDataTransferAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-storage:StartObject",
        "backup-storage:PutChunk",
        "backup-storage:GetChunk",
        "backup-storage:ListChunks",
        "backup-storage:ListObjects",
        "backup-storage:GetObjectMetadata",
        "backup-storage:NotifyObjectComplete"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBackupFullAccess

Deskripsi: Kebijakan ini untuk administrator cadangan, memberikan akses penuh ke operasi AWS Cadangan, termasuk membuat atau mengedit rencana cadangan, menetapkan AWS sumber daya untuk rencana cadangan, menghapus cadangan, dan memulihkan cadangan.

`AWSBackupFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 November 2019, 22:21 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupFullAccess`

Versi kebijakan

Versi kebijakan: v30 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsBackupAllAccessPermissions",
      "Effect" : "Allow",
      "Action" : "backup:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AwsBackupStorageAllAccessPermissions",
```

```
      "Effect" : "Allow",
      "Action" : "backup-storage:*",
      "Resource" : "*"
    },
    {
      "Sid" : "RdsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:describeDBEngineVersions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describeDBSubnetGroups",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBClusters",
        "rds:describeDBParameterGroups",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RdsDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBSnapshot",
        "rds:DeleteDBClusterSnapshot"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DynamoDbPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "dynamodb:ListBackups",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDbDeleteBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DeleteBackup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EfsFileSystemPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFilesystems"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "Ec2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:describeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcEndpoints",
```

```
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2DeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:DeregisterImage"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ResourceGroupTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StorageGatewayVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListGateways"
```

```
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Sid" : "StorageGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListLocalDisks"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "StorageGatewayGatewayStarPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackup*",
        "arn:aws:iam::*:role/*AWSBackup*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "backup.amazonaws.com",
            "restore-testing.backup.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AwsOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Sid" : "KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:backup:backup-vault"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "backup.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SystemManagerCommandPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SystemManagerSendCommandPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:DescribeBackups",
        "fsx:DescribeVolumes",
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DeleteBackup",
      "Resource" : "arn:aws:fsx:*:*:backup/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DirectoryServicePermissions",
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Sid" : "IamCreateServiceLinkedRolePermissions",
```

```
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "backup.amazonaws.com",
            "restore-testing.backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "BackupGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:AssociateGatewayToServer",
        "backup-gateway:CreateGateway",
        "backup-gateway:DeleteGateway",
        "backup-gateway:DeleteHypervisor",
        "backup-gateway:DisassociateGatewayFromServer",
        "backup-gateway:ImportHypervisorConfiguration",
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup-gateway:PutMaintenanceStartTime",
        "backup-gateway:TagResource",
        "backup-gateway:TestHypervisorConfiguration",
        "backup-gateway:UntagResource",
        "backup-gateway:UpdateGatewayInformation",
        "backup-gateway:UpdateHypervisor"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupGatewayHypervisorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings",
        "backup-gateway:PutHypervisorPropertyMappings",
        "backup-gateway:StartVirtualMachinesMetadataSync"
      ],
```

```
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "BackupGatewayVirtualMachinePermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetVirtualMachine"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "BackupGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway",
        "backup-gateway:PutBandwidthRateLimitSchedule"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:gateway/*"
    },
    {
      "Sid" : "CloudWatchPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListTables",
        "timestream:ListDatabases"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "S3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "RedshiftResourcesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeSnapshotSchedules"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:subnetgroup:*",
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:snapshotschedule:*"
      ]
    },
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeNodeConfigurationOptions",
        "redshift:DescribeOrderableClusterOptions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterTracks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListWorkgroups"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessDeletetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudFormationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
```

```
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Sid" : "SystemsManagerForSapPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceAccessManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DSQLDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
```

```
      "Sid" : "IamPassRolePermissionsForGuardDuty",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackupGuardDuty*",
        "arn:aws:iam::*:role/*AWSBackupGuardDuty*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

Deskripsi: Memberikan AWS BackupGateway izin untuk menyinkronkan metadata Mesin Virtual atas nama Anda

`AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 15 Desember 2022, 19:43 UTC
- Waktu teredit: 15 Desember 2022 19.43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListVmTags",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "VMTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:TagResource",
        "backup-gateway:UntagResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBackupGuardDutyRolePolicyForScans

Deskripsi: Memberikan GuardDuty izin untuk membaca AWS Backup Recovery Points untuk pemindaian malware

`AWSBackupGuardDutyRolePolicyForScans`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupGuardDutyRolePolicyForScans` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 November 2025, 03:34 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupGuardDutyRolePolicyForScans`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSDirectReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:ListChangedBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        },
        "StringLike" : {
          "aws:ResourceTag/aws:backup:source-resource" : "*"
        }
      }
    },
    {
      "Sid" : "CreateGrantForEncryptedVolumeCreation",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:guardduty:id" : "snap-*",
          "kms:ViaService" : [
            "guardduty.*.amazonaws.com",
            "backup.*.amazonaws.com"
          ]
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "CreateGrant",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo",
            "RetireGrant",
            "DescribeKey"
          ]
        },
```

```
        "Null" : {
          "kms:GrantOperations" : "false"
        }
      }
    },
    {
      "Sid" : "CreateGrantForReEncryptAndEBSDirect",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : "snap-*",
          "kms:ViaService" : [
            "guardduty.*.amazonaws.com",
            "backup.*.amazonaws.com"
          ]
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "RetireGrant",
            "DescribeKey"
          ]
        },
        "Null" : {
          "kms:GrantOperations" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeKeyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "EC2ReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ShareSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        },
        "StringLike" : {
          "aws:ResourceTag/aws:backup:source-resource" : "*"
        }
      }
    },
    {
      "Sid" : "ShareSnapshotKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : [
            "vol-*",
            "snap-*"
          ],
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateBackupAccessPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupAccessPoint"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*"
```

```
    },
    {
      "Sid" : "ReadAndDeleteBackupAccessPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeBackupAccessPoint",
        "backup:DeleteBackupAccessPoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupRecoveryPointApiPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeRecoveryPoint"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*"
    },
    {
      "Sid" : "DecryptKMSEncryptedDataByAWSBackup",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:backup:backup-vault" : "*",
          "kms:ViaService" : "backup.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBackupOperatorAccess

Deskripsi: Kebijakan ini memberikan izin kepada pengguna untuk menetapkan AWS sumber daya ke rencana cadangan, membuat cadangan sesuai permintaan, dan memulihkan cadangan. Kebijakan ini tidak mengizinkan pengguna untuk membuat atau mengedit rencana cadangan atau menghapus cadangan terjadwal setelah dibuat.

`AWSBackupOperatorAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupOperatorAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 November 2019, 22:23 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOperatorAccess`

Versi kebijakan

Versi kebijakan: v28 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsBackupAllAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup:Get*",
        "backup:List*",
        "backup:Describe*",
```

```
        "backup:CreateBackupSelection",
        "backup:DeleteBackupSelection",
        "backup:StartBackupJob",
        "backup:StartRestoreJob",
        "backup:StartCopyJob",
        "backup:StartScanJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:describeDBEngineVersions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describeDBSubnetGroups",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBAccess",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListBackups",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EFSAccess",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFilesystems"
      ],
```

```
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "EC2Access",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:describeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StorageGatewaySCSIAccess",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayReadAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "storagegateway:ListGateways"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Sid" : "StorageGatewayDiskReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListLocalDisks"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "StorageGatewayVolumeReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackup*",
        "arn:aws:iam::*:role/*AWSBackup*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMComandAccess",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "FSXDescribeAccess",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FSxFileAccess",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeFileSystems",
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Sid" : "FSxVolumeAccess",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeVolumes",
      "Resource" : "arn:aws:fsx:*:*:volume/*/*"
    },
    {
```

```
      "Sid" : "FSxMachineAccess",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeStorageVirtualMachines",
      "Resource" : "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
    },
    {
      "Sid" : "DirectoryServiceAccess",
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Sid" : "BackupGatewayListAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupGatewayHypervisorAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "BackupGatewayMachineAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetVirtualMachine"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "BackupGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetBandwidthRateLimitSchedule",
```

```
        "backup-gateway:GetGateway"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:gateway/*"
    },
    {
      "Sid" : "CloudWatchAccess",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamListAccess",
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListDatabases",
        "timestream:ListTables"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ListAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "RedshiftAccess",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusterSnapshots",
```

```
        "redshift:DescribeSnapshotSchedules"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:subnetgroup:*",
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:snapshotschedule:*"
      ]
    },
    {
      "Sid" : "RedshiftOptionsAccess",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeNodeConfigurationOptions",
        "redshift:DescribeOrderableClusterOptions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterTracks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
```

```
      ]
    },
    {
      "Sid" : "CloudFormationAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Sid" : "SAPAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SAPDatabaseAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    },
    {
      "Sid" : "RAMAccess",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DSQLDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters",
```

```
        "dsql:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "IamPassRolePermissionsForGuardDuty",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackupGuardDuty*",
        "arn:aws:iam::*:role/*AWSBackupGuardDuty*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBackupOrganizationAdminAccess

Deskripsi: Kebijakan ini untuk administrator cadangan yang menggunakan manajemen pencadangan lintas akun untuk mengelola cadangan untuk organisasi.

`AWSBackupOrganizationAdminAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupOrganizationAdminAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2020, 16:23 UTC
- Waktu teredit: 18 November 2022 18.26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DisableAWSServiceAccess",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:account/*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:AttachPolicy",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:DetachPolicy",
        "organizations:DisablePolicyType",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListPolicies",
        "organizations:EnablePolicyType",
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:PolicyType" : [
            "BACKUP_POLICY"
```

```
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBackupRestoreAccessForSAPHANA

Deskripsi: AWS Memberikan izin Cadangan untuk memulihkan cadangan SAP HANA di Amazon EC2

`AWSBackupRestoreAccessForSAPHANA`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupRestoreAccessForSAPHANA` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 November 2022, 22:43 UTC
- Waktu teredit: 10 November 2022, 22.43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupRestoreAccessForSAPHANA`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:Get*",
        "backup:List*",
        "backup:Describe*",
        "backup:StartBackupJob",
        "backup:StartRestoreJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:BackupDatabase",
        "ssm-sap:RestoreDatabase",
        "ssm-sap:UpdateHanaBackupSettings",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBackupSearchOperatorAccess

Deskripsi: Peran operator pencarian memiliki akses untuk membuat indeks cadangan, membuat pencarian metadata cadangan yang telah diindeks. Kebijakan ini berisi izin yang diperlukan untuk fungsi operator pencarian ini.

`AWSBackupSearchOperatorAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupSearchOperatorAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Februari 2025, 21:52 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC

- ARN: `arn:aws:iam::aws:policy/AWSBackupSearchOperatorAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartSearchAndListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-search:StartSearchJob",
        "backup-search:ListSearchJobs",
        "backup-search:ListSearchResultExportJobs",
        "backup:ListIndexedRecoveryPointsForSearch"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupSearchRecoveryPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:SearchRecoveryPoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:backup:*:*:recovery-point:*"
      ]
    },
    {
      "Sid" : "SearchAndExportPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-search:StartSearchResultExportJob",
```

```
        "backup-search:StopSearchJob",
        "backup-search:GetSearchJob",
        "backup-search:GetSearchResultExportJob",
        "backup-search:ListSearchJobResults",
        "backup-search:ListSearchJobBackups"
      ],
      "Resource" : [
        "arn:aws:backup-search:*:*:search-job/*",
        "arn:aws:backup-search:*:*:search-export-job/*"
      ]
    },
    {
      "Sid" : "KMSDataKeyForSearchAndExportPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:EncryptionContextKeys" : [
            "aws:backup-search:search-job"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : [
            "backup.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBackupServiceLinkedRolePolicyForBackup

Deskripsi: Mem AWS berikan izin Cadangan untuk membuat cadangan atas nama Anda di seluruh AWS layanan

`AWSBackupServiceLinkedRolePolicyForBackup`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 02 Juni 2020, 23:08 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup`

Versi kebijakan

Versi kebijakan: v31 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EFSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
```

```
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
        }
      }
    },
    {
      "Sid" : "DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "elasticfilesystem:DescribeFileSystems",
        "dynamodb:ListTables",
        "storagegateway:ListVolumes",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstances",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnapshotCopyTagPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CopySnapshot"
        }
      }
    },
    {
      "Sid" : "EC2CreateBackupTagPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
```

```
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AWSBackupManagedResource"
          ]
        }
      }
    },
    {
      "Sid" : "EC2CreateTagsPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSBackupManagedResource" : "false"
        }
      }
    },
    {
      "Sid" : "EC2RDSDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeImages",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBClusterSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EBSCopyPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CopySnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2CopyPermissions",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:CopyImage",
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeregisterImage",
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotTier"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSBackupManagedResource" : "false"
        }
      }
    },
    {
      "Sid" : "RDSInstanceAndSnashotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CopyDBSnapshot",
        "rds:DeleteDBSnapshot",
        "rds:DeleteDBInstanceAutomatedBackup"
      ],
      "Resource" : "arn:aws:rds:*:*:snapshot:awsbackup:*"
    },
    {
      "Sid" : "RDSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CopyDBClusterSnapshot",
        "rds:DeleteDBClusterSnapshot"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
    },
    {
      "Sid" : "RDSSnapshotTenantDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource"
```

```
      ],
      "Resource" : [
        "arn:aws:rds:*:*:snapshot-tenant-database:awsbackup:*"
      ]
    },
    {
      "Sid" : "KMSDescribePermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "fsx.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "fsx.*.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CopyBackup",
        "fsx:TagResource",
        "fsx:DescribeBackups",
        "fsx:DeleteBackup"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "DynamoDBDeletePermissions",
      "Effect" : "Allow",
      "Action" : "dynamodb:DeleteBackup",
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "BackupGateway",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListTagsForBackupGateway",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTagsOfResource",
        "dynamodb:DescribeTable"
      ],
```

```
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "EventBridgePermissions",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:PutRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule",
        "events:DisableRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
      ]
    },
    {
      "Sid" : "EventBridgeRulesPermissions",
      "Effect" : "Allow",
      "Action" : "events:ListRules",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:UpdateHANABackupSettings"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:DescribeDatabase",
        "timestream:DescribeTable",
        "timestream:GetAwsBackupStatus",
        "timestream:GetAwsRestoreStatus"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftClusterSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DeleteClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
```

```
    },
    {
      "Sid" : "RedshiftClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessDeleteSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudformationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Sid" : "RecoveryPointTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:TagResource"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "DSQLListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrgsListDelegatedAdmins",
      "Effect" : "Allow",
```

```
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EKSClusterConfigurationBackup",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster",
        "eks:ListAddons",
        "eks:DescribeAddon",
        "eks:ListNodegroups",
        "eks:DescribeNodegroup",
        "eks:ListPodIdentityAssociations",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:DescribeAccessEntry",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListFargateProfiles",
        "eks:DescribeFargateProfile",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBackupServiceLinkedRolePolicyForBackupTest

Deskripsi: Mem AWS berikan izin Cadangan untuk membuat cadangan atas nama Anda di seluruh AWS layanan

`AWSBackupServiceLinkedRolePolicyForBackupTest`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 12 Mei 2020, 17:37 UTC
- Waktu teredit: 12 Mei 2020, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
```

```
      "Effect" : "Allow",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
        }
      }
    },
    {
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBackupServiceRolePolicyForBackup

Deskripsi: Mem AWS berikan izin Cadangan untuk membuat cadangan atas nama Anda di seluruh AWS layanan

`AWSBackupServiceRolePolicyForBackup`padalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupServiceRolePolicyForBackup` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 10 Januari 2019, 21:01 UTC
- Waktu teredit: 23 Februari 2026, 19:42 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup`

Versi kebijakan

Versi kebijakan: v30 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:CreateBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeBackup",
        "dynamodb:DeleteBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "DynamoDBBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:ListTagsForResource",
        "rds:DescribeDBSnapshots",
        "rds:CreateDBSnapshot",
```

```
        "rds:CopyDBSnapshot",
        "rds:DescribeDBInstances",
        "rds:CreateDBClusterSnapshot",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshots",
        "rds:CopyDBClusterSnapshot",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSInstanceAutomatedBackupPermissions",
      "Effect" : "Allow",
      "Action" : "rds:DeleteDBInstanceAutomatedBackup",
      "Resource" : "arn:aws:rds:*:*:auto-backup:*"
    },
    {
      "Sid" : "RDSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:ModifyDBCluster"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RDSClusterBackupPermissions",
      "Effect" : "Allow",
      "Action" : "rds:DeleteDBClusterAutomatedBackup",
      "Resource" : "arn:aws:rds:*:*:cluster-auto-backup:*"
    },
    {
      "Sid" : "RDSModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:ModifyDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*"
      ]
    },
    {
      "Sid" : "RDSBackupPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBSnapshot",
        "rds:ModifyDBSnapshotAttribute"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:snapshot:awsbackup:*"
      ]
    },
    {
      "Sid" : "RDSClusterModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBClusterSnapshot",
        "rds:ModifyDBClusterSnapshotAttribute"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
      ]
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:CreateSnapshot",
        "storagegateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "EBSCopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2CopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "EBSTagAndDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeElasticGpus",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSnapshotTierStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:image/*"
    },
    {
      "Sid" : "EC2ModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:ModifyImageAttribute"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "EBSSnapshotTierPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotTier"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "BackupVaultPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeBackupVault",
        "backup:CopyIntoBackupVault"
      ],
      "Resource" : "arn:aws:backup:*:*:backup-vault:*"
    },
    {
      "Sid" : "BackupVaultCopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:CopyFromBackupVault"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
```

```
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "EBSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSDynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dynamodb.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "KMSEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:ebs:id"
        }
      }
    },
    {
      "Sid" : "GetResourcesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSendPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
```

```
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "FsxBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxCreateBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:CreateBackup",
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeFileSystems",
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Sid" : "FsxVolumePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeVolumes",
      "Resource" : "arn:aws:fsx:*:*:volume/*"
    },
    {
      "Sid" : "FsxListTagsPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:ListTagsForResource",
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
```

```
      "Action" : "fsx:DeleteBackup",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:CopyBackup",
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "DynamodbBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:StartAwsBackupJob",
        "dynamodb:ListTagsOfResource"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "BackupGatewayBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:Backup",
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "CloudformationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:GetTemplate",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/*/*"
    },
    {
```

```
      "Sid" : "RedshiftCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateClusterSnapshot",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DeleteClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessCreatePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*",
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:TagResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
```

```
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:StartAwsBackupJob",
        "timestream:GetAwsBackupStatus",
        "timestream:ListTables",
        "timestream:ListDatabases",
        "timestream:ListTagsForResource",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:BackupDatabase",
        "ssm-sap:UpdateHanaBackupSettings",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    },
    {
      "Sid" : "RecoveryPointTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:TagResource"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "DSQLResourcePermissionsForBackup",
      "Effect" : "Allow",
      "Action" : [
        "dsql:StartBackupJob",
        "dsql:GetBackupJob",
        "dsql:StopBackupJob",
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "KMSDSQLPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:dsql:ClusterId"
        }
      }
    },
    {
      "Sid" : "EKSClusterConfigurationBackup",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster",
        "eks:ListAddons",
        "eks:DescribeAddon",
        "eks:ListNodegroups",
        "eks:DescribeNodegroup",
        "eks:ListPodIdentityAssociations",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:DescribeAccessEntry",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListFargateProfiles",
        "eks:DescribeFargateProfile",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateBackupAccessEntry",
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateAccessEntry"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
```

```
    },
    {
      "Sid" : "AssociateBackupAccessPolicy",
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DisassociateAccessPolicy"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*",
      "Condition" : {
        "StringEquals" : {
          "eks:policyArn" : "arn:aws:eks::aws:cluster-access-policy/
AWSBackupFullAccessPolicyForBackup",
          "eks:accessScope" : "cluster"
        }
      }
    },
    {
      "Sid" : "GuardDutyMalwareScanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:StartMalwareScan",
        "guardduty:GetMalwareScan"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyMalwareScanIAMPassPermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBackupServiceRolePolicyForIndexing

Deskripsi: Kebijakan berisi izin yang diperlukan untuk AWS Backup untuk mengindeks titik pemulihan.

`AWSBackupServiceRolePolicyForIndexing`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupServiceRolePolicyForIndexing` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Desember 2024, 18:37 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForIndexing`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSReadOnlyPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "EBSDirectReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "KMSDataKeyForEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBackupServiceRolePolicyForItemRestores

Deskripsi: Kebijakan berisi izin yang diperlukan untuk AWS Cadangan untuk memulihkan item individual di titik pemulihan

`AWSBackupServiceRolePolicyForItemRestores`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupServiceRolePolicyForItemRestores` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Desember 2024, 18:37 UTC
- Waktu teredit: 12 Februari 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForItemRestores`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSReadOnlyPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "EBSDirectReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "S3ReadonlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3PermissionsForFileLevelRestore",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : "arn:aws:s3:::*/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSDataKeyForS3AndEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
            "s3.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBackupServiceRolePolicyForRestores

Deskripsi: Mem AWS berikan izin Cadangan untuk melakukan pemulihan atas nama Anda di seluruh AWS layanan. Kebijakan ini mencakup izin untuk membuat dan menghapus AWS sumber daya, seperti volume EBS, instans RDS, dan sistem file EFS, yang merupakan bagian dari proses pemulihan.

`AWSBackupServiceRolePolicyForRestores`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupServiceRolePolicyForRestores` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 12 Januari 2019, 00:23 UTC
- Waktu teredit: 27 Agustus 2026, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForRestores`

Versi kebijakan

Versi kebijakan: v36 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:PutItem",
        "dynamodb:GetItem",
        "dynamodb:DeleteItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
```

```
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:RestoreTableFromBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "EBSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "EC2DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateTagsPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonFSx" : "ManagedByAmazonFSx"
        }
      }
    },
    {
      "Sid" : "StorageGatewayVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DeleteVolume",
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes",
        "storagegateway:AddTagsToResource"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:CreateStorediSCSIVolume",
        "storagegateway:CreateCachediSCSIVolume"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "StorageGatewayListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Sid" : "RDSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
```

```
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:RestoreDBInstanceFromDBSnapshot",
        "rds:DeleteDBInstance",
        "rds:AddTagsToResource",
        "rds:DescribeDBClusters",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:DeleteDBCluster",
        "rds:RestoreDBInstanceToPointInTime",
        "rds:DescribeDBClusterSnapshots",
        "rds:RestoreDBClusterToPointInTime",
        "rds:CreateTenantDatabase",
        "rds:DeleteTenantDatabase"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Restore",
        "elasticfilesystem:CreateFilesystem",
        "elasticfilesystem:DescribeFilesystems",
        "elasticfilesystem:DeleteFilesystem",
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "KMSDescribePermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "DSQLResourcePermissionsForRestore",
      "Effect" : "Allow",
      "Action" : [
        "dsql:StartRestoreJob",
        "dsql:GetRestoreJob",
        "dsql:StopRestoreJob",
        "dsql:TagResource",
        "dsql:CreateCluster",
        "dsql:PutMultiRegionProperties",
```

```
        "dsql:PutWitnessRegion",
        "dsql:UpdateCluster",
        "dsql:AddPeerCluster",
        "dsql:RemovePeerCluster",
        "dsql:GetCluster"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dynamodb.*.amazonaws.com",
            "ec2.*.amazonaws.com",
            "elasticfilesystem.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "dsql.*.amazonaws.com",
            "redshift-serverless.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
```

```
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "EBSSnapshotBlockPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:CompleteSnapshot",
        "ebs:StartSnapshot",
        "ebs:PutSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "RDSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBInstance"
      ],
      "Resource" : "arn:aws:rds:*:*:db:*"
    },
    {
      "Sid" : "EC2DeleteAndRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:DeleteTags",
        "ec2:RestoreSnapshotTier"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "EC2CreateTagsScopedPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
```

```
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:backup:source-resource"
          ]
        }
      }
    },
    {
      "Sid" : "EC2RunInstancesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TerminateInstancesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "EC2CreateTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateVolume"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateFileSystemFromBackup"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:backup/*"
      ]
    },
    {
      "Sid" : "FsxTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Sid" : "FsxBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteFileSystem",
        "fsx:UntagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:file-system/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "FsxDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "fsx:DescribeVolumes"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*"
    },
    {
      "Sid" : "FsxVolumeTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateVolumeFromBackup",
        "fsx:TagResource"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:volume/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:backup:source-resource"
          ]
        }
      }
    },
    {
      "Sid" : "FsxBackupTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateVolumeFromBackup",
        "fsx:TagResource"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:storage-virtual-machine/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteVolume",
        "fsx:UntagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*",
      "Condition" : {
```

```
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "DSPermissions",
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:RestoreTableFromAwsBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "GatewayRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:Restore"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "CloudformationChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:*/*/*"
    },
    {
      "Sid" : "RedshiftClusterSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:RestoreFromClusterSnapshot",
        "redshift:RestoreTableFromClusterSnapshot"
```

```
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftTablePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeTableRestoreStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftServerlessSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:RestoreTableFromSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessNamespacePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace"
      ],
      "Resource" : [
```

```
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessTablePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetTableRestoreStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:StartAwsRestoreJob",
        "timestream:GetAwsRestoreStatus",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:ListDatabases",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EKSClusterRestore",
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateCluster",
```

```
        "eks:DescribeCluster",
        "eks:CreateAccessEntry",
        "eks:DescribeAccessEntry",
        "eks:AssociateAccessPolicy",
        "eks:ListAssociatedAccessPolicies",
        "eks:CreateAddon",
        "eks:DescribeAddon",
        "eks:CreateNodegroup",
        "eks:DescribeNodegroup",
        "eks:CreateFargateProfile",
        "eks:DescribeFargateProfile",
        "eks:CreatePodIdentityAssociation",
        "eks:DescribePodIdentityAssociation",
        "eks:TagResource"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:access-entry/*",
        "arn:aws:eks:*:*:addon/*",
        "arn:aws:eks:*:*:cluster/*",
        "arn:aws:eks:*:*:fargateprofile/*",
        "arn:aws:eks:*:*:nodegroup/*",
        "arn:aws:eks:*:*:podidentityassociation/*"
      ]
    },
    {
      "Sid" : "AssociateRestoreAccessPolicy",
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DisassociateAccessPolicy"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*",
      "Condition" : {
        "StringEquals" : {
          "eks:accessScope" : "cluster",
          "eks:policyArn" : "arn:aws:eks::aws:cluster-access-policy/
AWSBackupFullAccessPolicyForRestore"
        }
      }
    },
    {
      "Sid" : "CreateClusterIAMPerms",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "eks.amazonaws.com",
            "ec2.amazonaws.com",
            "pods.eks.amazonaws.com",
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateEKSNodeGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSubnets",
        "ec2:RunInstances",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSNodeGroupTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "BackupRestoreJobManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:StartRestoreJob",
        "backup:ListRestoreJobs",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:DescribeRestoreJob"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBackupServiceRolePolicyForS3Backup

Deskripsi: Kebijakan yang berisi izin yang diperlukan untuk AWS Backup untuk mencadangkan data di bucket S3 apa pun. Ini termasuk akses baca ke semua objek S3 dan akses dekripsi apa pun untuk semua kunci KMS.

`AWSBackupServiceRolePolicyForS3Backup`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupServiceRolePolicyForS3Backup` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Februari 2022, 17:40 UTC

- Waktu teredit: 24 Agustus 2026, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchGetMetricDataPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridgePermissionsForAwsBackupManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:PutRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule",
        "events:DisableRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
      ]
    },
    {
      "Sid" : "EventBridgeListRulesPermissions",
      "Effect" : "Allow",
```

```
      "Action" : "events:ListRules",
      "Resource" : "*"
    },
    {
      "Sid" : "KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketTagging",
        "s3:GetInventoryConfiguration",
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:GetBucketLocation",
        "s3:GetBucketAcl",
        "s3:PutInventoryConfiguration",
        "s3:GetBucketNotification",
        "s3:PutBucketNotification"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "S3ObjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectAcl",
        "s3:GetObject",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion"
```

```
      ],
      "Resource" : "arn:aws:s3:::*/*"
    },
    {
      "Sid" : "S3ListBucketPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListAllMyBuckets",
      "Resource" : "*"
    },
    {
      "Sid" : "S3BucketTagReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListTagsForResource"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "RecoveryPointTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:TagResource"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBackupServiceRolePolicyForS3Restore

Deskripsi: Kebijakan berisi izin yang diperlukan untuk AWS Backup untuk memulihkan cadangan S3 ke bucket. Ini termasuk read/write izin ke semua bucket S3, dan izin ke GenerateDataKey dan DescribeKey untuk semua kunci KMS.

`AWSBackupServiceRolePolicyForS3Restore`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupServiceRolePolicyForS3Restore` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Februari 2022, 17:39 UTC
- Waktu teredit: 07 Februari 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:GetBucketLocation",
        "s3:PutBucketVersioning",
        "s3:PutBucketOwnershipControls",
        "s3:GetBucketOwnershipControls"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:DeleteObject",
        "s3:PutObjectVersionAcl",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging",
        "s3:GetObjectAcl",
        "s3:PutObjectAcl",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBackupServiceRolePolicyForScans

Deskripsi: Memberikan izin AWS Cadangan untuk melakukan pemindaian malware pada Poin Pem AWS ulihan Cadangan Anda

`AWSBackupServiceRolePolicyForScans`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupServiceRolePolicyForScans` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 November 2025, 03:34 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForScans`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyMalwareScanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:StartMalwareScan",
        "guardduty:GetMalwareScan"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassPermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2ReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBatchFullAccess

Deskripsi: Menyediakan akses penuh untuk sumber daya AWS Batch.

`AWSBatchFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBatchFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Desember 2016, 19:35 UTC
- Waktu teredit: 24 Oktober 2022, 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBatchFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "batch:*",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeImages",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ecs:DescribeClusters",
        "ecs:Describe*",
        "ecs:List*",
        "eks:DescribeCluster",
        "eks:ListClusters",
        "logs:Describe*",
        "logs:Get*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSBatchServiceRole",
        "arn:aws:iam::*:role/service-role/AWSBatchServiceRole",
        "arn:aws:iam::*:role/ecsInstanceRole",
        "arn:aws:iam::*:instance-profile/ecsInstanceRole",
        "arn:aws:iam::*:role/iaws-ec2-spot-fleet-role",
        "arn:aws:iam::*:role/aws-ec2-spot-fleet-role",
        "arn:aws:iam::*:role/AWSBatchJobRole*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/*Batch*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "batch.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBatchServiceEventTargetRole

Deskripsi: Kebijakan untuk mengaktifkan Target CloudWatch Peristiwa untuk Pen AWS giriman Pekerjaan Batch

`AWSBatchServiceEventTargetRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBatchServiceEventTargetRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 28 Februari 2018, 22:31 UTC
- Waktu teredit: 28 Februari 2018, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceEventTargetRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "batch:SubmitJob"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBatchServiceRole

Deskripsi: Kebijakan untuk peran layanan AWS Batch yang memungkinkan akses ke layanan terkait termasuk EC2, Autoscaling, layanan Kontainer EC2, dan Cloudwatch Logs.

`AWSBatchServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBatchServiceRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Desember 2016, 19:36 UTC
- Waktu teredit: 25 Agustus 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole`

Versi kebijakan

Versi kebijakan: v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBatchPolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeImages",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
```

```
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:CreateLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:RequestSpotFleet",
        "ec2:CancelSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "ec2:TerminateInstances",
        "ec2:RunInstances",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:SuspendProcesses",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTasks",
        "ecs:ListAccountSettings",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "ecs:ListTasks",
        "ecs:CreateCluster",
        "ecs:DeleteCluster",
        "ecs:RegisterTaskDefinition",
        "ecs:DeregisterTaskDefinition",
        "ecs:RunTask",
        "ecs:StartTask",
        "ecs:StopTask",
        "ecs:UpdateCluster",
```

```
        "ecs:UpdateContainerAgent",
        "ecs:DeregisterContainerInstance",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "iam:GetInstanceProfile",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement2",
      "Effect" : "Allow",
      "Action" : "ecs:TagResource",
      "Resource" : [
        "arn:aws:ecs:*:*:task/*_Batch_*"
      ]
    },
    {
      "Sid" : "AWSBatchPolicyStatement3",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "ecs-tasks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement4",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
```

```
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "autoscaling.amazonaws.com",
            "ecs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement5",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBatchServiceRolePolicyForSageMaker

Deskripsi: Menyediakan akses AWS Batch untuk mengantri dan mengelola beban SageMaker kerja Amazon

`AWSBatchServiceRolePolicyForSageMaker`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 15 Juli 2025, 21:37 UTC
- Waktu teredit: 16 April 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBatchServiceRolePolicyForSageMaker`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:ListTags",
        "sagemaker:DeleteTrainingJob"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:training-job/AWSBatch*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:CreateTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:training-job/AWSBatch*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : "CreateTrainingJob"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTrainingJobs",
        "sagemaker:Search"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBCMDataExportsServiceRolePolicy

Deskripsi: Peran terkait layanan untuk menyediakan akses Ekspor Data Manajemen Penagihan dan Biaya ke data AWS layanan untuk mengekspor data ke lokasi target, seperti Amazon S3, atas nama pelanggan.

`AWSBCMDataExportsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 10 Juni 2024, 17:40 UTC
- Waktu teredit: 10 Juni 2024, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBCMDataExportsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationRecommendationAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBedrockAgentCoreGatewayNetworkServiceRolePolicy

Deskripsi: Mengizinkan Bedrock AgentCore Gateway mengelola sumber daya VPC Lattice atas nama Anda

`AWSBedrockAgentCoreGatewayNetworkServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 28 Maret 2026, 22:12 UTC
- Waktu teredit: 28 Maret 2026, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBedrockAgentCoreGatewayNetworkServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSLRActionsForLattice",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "vpc-lattice.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowResourceGatewayCreate",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:CreateResourceGateway",
        "vpc-lattice:TagResource"
      ],
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:resourcegateway/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/BedrockAgentCoreGatewayManaged" : "true",
          "aws:ResourceTag/BedrockAgentCoreGatewayManaged" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "AllowEC2PermissionsForResourceGatewayCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowResourceGatewayDelete",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:DeleteResourceGateway",
        "vpc-lattice:GetResourceGateway"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/BedrockAgentCoreGatewayManaged" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBedrockAgentCoreIdentityNetworkServiceRolePolicy

Deskripsi: Mengizinkan AgentCore Identitas Bedrock untuk mengelola sumber daya VPC Lattice atas nama Anda

`AWSBedrockAgentCoreIdentityNetworkServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 15 April 2026, 00:42 UTC
- Waktu teredit: 15 April 2026, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBedrockAgentCoreIdentityNetworkServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSLRActionsForLattice",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "vpc-lattice.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowResourceGatewayCreate",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:CreateResourceGateway",
        "vpc-lattice:TagResource"
      ],
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:resourcegateway/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/BedrockAgentCoreIdentityManaged" : "true",
          "aws:ResourceTag/BedrockAgentCoreIdentityManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowEC2PermissionsForResourceGatewayCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowResourceGatewayDelete",
      "Effect" : "Allow",
      "Action" : [
```

```
        "vpc-lattice:DeleteResourceGateway",
        "vpc-lattice:GetResourceGateway"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/BedrockAgentCoreIdentityManaged" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBedrockAgentCoreRuntimeInstancesServiceRolePolicy

Deskripsi: Mengizinkan Instans AgentCore Runtime Bedrock mengelola sumber daya komputasi atas nama Anda.

`AWSBedrockAgentCoreRuntimeInstancesServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 05 Agustus 2026, 09:57 UTC
- Waktu teredit: 05 Agustus 2026, 09:57 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBedrockAgentCoreRuntimeInstancesServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDescribeResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowCleanupManagedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:ManagedResourceOperator" : "bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCleanupAutoScalingGroup",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:CompleteLifecycleAction"
      ],
      "Resource" : "arn:aws:autoscaling:*:*:autoScalingGroup:*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/bedrock-agentcore:capacity-provider-id" : "false"
        }
      }
    },
    {
      "Sid" : "AllowCleanupEventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCleanupEBSVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "bedrock-agentcore.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "AllowDetachEBSVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowTerminateManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "bedrock-agentcore.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBillingConductorFullAccess

Deskripsi: Gunakan kebijakan AWSBillingConductorFullAccess terkelola untuk mengizinkan akses lengkap ke konsol AWS Billing Conductor (ABC) dan API. Kebijakan ini memungkinkan pengguna untuk membuat daftar, membuat, dan menghapus sumber daya ABC.

`AWSBillingConductorFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBillingConductorFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 April 2022, 18:02 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:*",
        "organizations:ListAccounts",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
```

```
        "pricing:GetProducts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:DescribeResponsibilityTransfer",
        "organizations:ListInboundResponsibilityTransfers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBillingConductorReadOnlyAccess

Deskripsi: Gunakan kebijakan AWSBillingConductorReadOnlyAccess terkelola untuk mengizinkan akses baca saja ke konsol AWS Billing Conductor (ABC) dan API. Kebijakan ini memberikan izin untuk melihat dan mencantumkan semua sumber daya ABC. Itu tidak termasuk kemampuan untuk membuat atau menghapus sumber daya.

`AWSBillingConductorReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBillingConductorReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 April 2022, 18:02 UTC
- Waktu teredit: 21 September 2026, 18:17 UTC

- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:List*",
        "billingconductor:GetBillingGroupCostReport",
        "billingconductor:GetBillingTransferPreference",
        "organizations:ListAccounts",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetProducts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:DescribeResponsibilityTransfer",
        "organizations:ListInboundResponsibilityTransfers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBillingConductorRolePolicy

Deskripsi: Menye AWS Billing Conductor diakan akses untuk mengelola grup penagihan dan sumber daya terkait

`AWSBillingConductorRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 21 September 2026, 19:07 UTC
- Waktu teredit: 21 September 2026, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBillingConductorRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : "billingconductor:CreateBillingGroup",
      "Resource" : [
        "arn:aws:billingconductor::*:billinggroup/*",
        "arn:aws:billingconductor::*:pricingplan/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "billingconductor:GetBillingTransferPreference",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "organizations:DescribeResponsibilityTransfer",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBillingReadOnlyAccess

Deskripsi: Memungkinkan pengguna untuk melihat tagihan di Konsol Penagihan.

`AWSBillingReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBillingReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Agustus 2020, 20:08 UTC
- Waktu teredit: 30 Juli 2026, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v28 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:ViewBilling",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetCredits",
        "billing:GetContractInformation",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "budgets:ViewBudget",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionHistories",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetCostAndUsage",
        "ce:ListCostCategoryDefinitions",
        "ce:ListCostCategoryResourceAssociations",
        "ce:ListTagsForResource",
        "ce:ListCostAllocationTags",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:GetTags",
        "ce:GetDimensionValues",
        "ce:GetCostAndUsageComparisons",
```

```
        "ce:GetCostComparisonDrivers",
        "consolidatedbilling:ListLinkedAccounts",
        "consolidatedbilling:GetAccountBillingRole",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "cur:DescribeReportDefinitions",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "freetier:GetAccountPlanState",
        "freetier:GetAccountActivity",
        "freetier:ListAccountActivities",
        "invoicing:BatchGetInvoiceProfile",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:GetInvoiceUnit",
        "invoicing:GetInvoiceCorrection",
        "invoicing:ListInvoiceSummaries",
        "invoicing:ListInvoiceUnits",
        "invoicing:GetProcurementPortalPreference",
        "invoicing:ListProcurementPortalPreferences",
        "invoicing:ListTagsForResource",
        "invoicing:ListInvoiceCorrections",
        "invoicing:ListProcurementPortals",
        "invoicing:ListProcurementPortalSuppliers",
        "mapcredits:ListQuarterSpend",
        "mapcredits:ListAssociatedPrograms",
        "mapcredits:ListQuarterCredits",
        "payments:GetFinancingApplication",
        "payments:GetFinancingLine",
        "payments:GetFinancingLineWithdrawal",
        "payments:GetFinancingOption",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListFinancingApplications",
        "payments:ListFinancingLines",
        "payments:ListFinancingLineWithdrawals",
        "payments:ListPaymentInstruments",
        "payments:ListPaymentPreferences",
        "payments:ListPaymentProgramOptions",
        "payments:ListPaymentProgramStatus",
        "payments:ListTagsForResource",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ViewPurchaseOrders",
```

```
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "sustainability:GetCarbonFootprintSummary",
        "tax:GetTaxRegistrationDocument",
        "tax:GetTaxInheritance",
        "tax:ListTaxRegistrations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBillingServiceRolePolicy

Deskripsi: Mengizinkan layanan penagihan untuk memvalidasi akses ke data tampilan penagihan untuk tampilan penagihan turunan

`AWSBillingServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 11 September 2025, 16:19 UTC
- Waktu teredit: 11 September 2025, 16:19 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBillingServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billing:GetBillingViewData"
      ],
      "Resource" : "arn:aws:billing::*:billingview/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

Deskripsi: Kebijakan ini memberikan izin untuk mengontrol AWS sumber daya. Misalnya, untuk memulai dan menghentikan instans EC2 atau RDS dengan menjalankan skrip AWS System Manager (SSM).

`AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Mei 2022, 19:03 UTC
- Waktu teredit: 07 April 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "rds:DescribeDBInstances",
        "rds:StartDBInstance",
        "rds:StopDBInstance"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-StartEC2Instance",
        "arn:aws:ssm:*:*:document/AWS-StopEC2Instance",
        "arn:aws:ssm:*:*:document/AWS-StartRdsInstance",
        "arn:aws:ssm:*:*:document/AWS-StopRdsInstance",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StartEC2Instance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopEC2Instance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StartRdsInstance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopRdsInstance:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBudgetsActionsWithAWSResourceControlAccess

Deskripsi: Menyediakan akses penuh ke AWS Tindakan Anggaran termasuk menggunakan Tindakan Anggaran untuk mengontrol status sumber AWS daya yang sedang berjalan melalui Konsol Manajemen AWS

`AWSBudgetsActionsWithAWSResourceControlAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBudgetsActionsWithAWSResourceControlAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Oktober 2020, 17:19 UTC
- Waktu teredit: 15 Oktober 2020, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActionsWithAWSResourceControlAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "budgets:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "budgets.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ModifyBilling",
        "ec2:DescribeInstances",
        "iam:ListGroups",
        "iam:ListPolicies",
        "iam:ListRoles",
        "iam:ListUsers",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListPolicies",
        "organizations:ListRoots",
        "rds:DescribeDBInstances",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBudgetsReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke AWS Konsol Anggaran melalui Konsol Manajemen AWS.

`AWSBudgetsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBudgetsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Oktober 2020, 17:18 UTC
- Waktu teredit: 17 Juni 2024, 17:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBudgetsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*",
        "budgets:ListTagsForResource"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBudgetsSpendLimitMemberRolePolicy

Deskripsi: Memberikan AWS izin layanan Anggaran untuk menjelaskan, menghentikan, dan menghentikan sumber daya di akun anggota untuk menerapkan tindakan batas pengeluaran.

`AWSBudgetsSpendLimitMemberRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: Juli 18, 2026, 00:57 UTC
- Waktu teredit: 13 Agustus 2026, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBudgetsSpendLimitMemberRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:StopInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeAddresses",
        "ec2:DescribeSnapshots",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSActions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:StopDBInstance",
        "rds:DescribeDBClusters",
        "rds:StopDBCluster",
        "rds:CreateDBClusterSnapshot",
        "rds:DescribeDBClusterSnapshots",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime",
        "rds:DescribeIntegrations",
        "rds:DescribeDBProxies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DSQLActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:ListNotebookInstances",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StartNotebookInstance",
        "sagemaker:DescribeApp",
        "sagemaker:ListApps",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:ListTrainingJobs",
        "sagemaker:StopTrainingJob",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:ListProcessingJobs",
        "sagemaker:StopProcessingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:StopTransformJob",
        "sagemaker:ListEndpoints",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:DescribeCluster",
        "sagemaker:ListClusters",
        "sagemaker:DescribeClusterNode",
        "sagemaker:ListClusterNodes",
        "sagemaker:AttachClusterNodeVolume",
        "sagemaker:DetachClusterNodeVolume",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:StopLabelingJob",
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "LambdaActions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
        "lambda:GetFunctionConcurrency",
        "lambda:PutFunctionConcurrency",
        "lambda:DeleteFunctionConcurrency",
        "lambda:ListEventSourceMappings",
        "lambda:GetEventSourceMapping",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:ListProvisionedConcurrencyConfigs",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:DeleteProvisionedConcurrencyConfig"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockActions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:ListProvisionedModelThroughputs",
        "bedrock:UpdateProvisionedModelThroughput",
        "bedrock:GetModelInvocationJob",
        "bedrock:ListModelInvocationJobs",
        "bedrock:StopModelInvocationJob",
        "bedrock:GetModelCustomizationJob",
        "bedrock:ListModelCustomizationJobs",
        "bedrock:StopModelCustomizationJob",
        "bedrock:GetEvaluationJob",
        "bedrock:ListEvaluationJobs",
        "bedrock:StopEvaluationJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:GetAutomationExecution",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions",
```

```
        "ssm:StopAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-StartEC2Instance",
        "arn:aws:ssm:*:*:document/AWS-StopEC2Instance",
        "arn:aws:ssm:*:*:document/AWS-StartRdsInstance",
        "arn:aws:ssm:*:*:document/AWS-StopRdsInstance",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StartEC2Instance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopEC2Instance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StartRdsInstance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopRdsInstance:*"
      ]
    },
    {
      "Sid" : "CostOptimizationHubActions",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:UpdateEnrollmentStatus",
        "cost-optimization-hub:ListEnrollmentStatuses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ComputeOptimizerActions",
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:GetIdleRecommendations",
        "compute-optimizer:GetRecommendationSummaries",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:UpdateEnrollmentStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ComputeOptimizerAutomationActions",
      "Effect" : "Allow",
      "Action" : [
        "aco-automation:StartAutomationEvent",
        "aco-automation:ListRecommendedActions",
        "aco-automation:GetAutomationEvent",
        "aco-automation:GetEnrollmentConfiguration",
```

```
        "aco-automation:UpdateEnrollmentConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOActions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccountActions",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetPrimaryEmail"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAWSServiceAccessForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "arn:aws:organizations:*:*:*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "cost-optimization-hub.bcm.amazonaws.com",
            "compute-optimizer.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowACOAutomationSLRCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/aco-automation.amazonaws.com/
AWSServiceRoleForComputeOptimizerAutomation",
      "Condition" : {
```

```
        "StringLike" : {
          "iam:AWSServiceName" : "aco-automation.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowComputeOptimizerSLRCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/cost-optimization-hub.bcm.amazonaws.com/
AWSServiceRoleForCostOptimizationHub",
        "arn:aws:iam::*:role/aws-service-role/compute-optimizer.amazonaws.com/
AWSServiceRoleForComputeOptimizer",
        "arn:aws:iam::*:role/aws-service-role/aco-automation.amazonaws.com/
AWSServiceRoleForComputeOptimizerAutomation"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "compute-optimizer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCostOptimizationHubSLRCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cost-optimization-
hub.bcm.amazonaws.com/AWSServiceRoleForCostOptimizationHub",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cost-optimization-hub.bcm.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBugBustFullAccess

Deskripsi: Kebijakan IAM ini memberi pengguna akses penuh ke konsol AWS BugBust

`AWSBugBustFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBugBustFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2021, 07:03 UTC
- Waktu teredit: 22 Juli 2021, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeGuruReviewerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:ListCodeReviews"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CodeGuruProfilerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-profiler:DescribeProfilingGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBugBustFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "bugbust:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBugBustSLRCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/bugbust.amazonaws.com/
AWSServiceRoleForBugBust",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "bugbust.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBugBustPlayerAccess

Deskripsi: Kebijakan IAM ini memberi pengguna akses untuk berpartisipasi dalam acara AWS BugBust

`AWSBugBustPlayerAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBugBustPlayerAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2021, 07:15 UTC
- Waktu teredit: 24 Juni 2021, 07:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustPlayerAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeGuruReviewerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListRecommendations"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CodeGuruProfilerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:DescribeProfilingGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBugBustPlayerAccess",
      "Effect" : "Allow",
      "Action" : [
        "bugbust:ListBugs",
        "bugbust:ListProfilingGroups",
        "bugbust:JoinEvent",
        "bugbust:GetEvent",
        "bugbust:ListEvents",
        "bugbust:GetJoinEventStatus",
        "bugbust:ListEventScores",
        "bugbust:ListEventParticipants",
        "bugbust:UpdateWorkItem",
        "bugbust:ListPullRequests"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSBugBustServiceRolePolicy

Deskripsi: Memberikan izin AWS BugBust untuk mengakses sumber daya atas nama Anda

`AWSBugBustServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 24 Juni 2021, 06:59 UTC
- Waktu teredit: 24 Juni 2021, 06:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:UntagResource",
        "codeguru-reviewer:DescribeCodeReview"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/bugbust" : "enabled"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCertificateManagerFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Certificate Manager (ACM)

`AWSCertificateManagerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCertificateManagerFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Januari 2016, 17:02 UTC
- Waktu teredit: 17 Agustus 2020, 22:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "acm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCertificateManagerPrivateCAAuditor

Deskripsi: Menyediakan akses auditor ke Otor AWS itas Sertifikat Pribadi Manajer Sertifikat

`AWSCertificateManagerPrivateCAAuditor`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCertificateManagerPrivateCAAuditor` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Oktober 2018, 16:51 UTC
- Waktu teredit: 17 Agustus 2020, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:CreateCertificateAuthorityAuditReport",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:GetPolicy",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags"
```

```
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCertificateManagerPrivateCAFullAccess

Deskripsi: Menyediakan akses penuh ke Otor AWS itas Sertifikat Pribadi Manajer Sertifikat

`AWSCertificateManagerPrivateCAFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCertificateManagerPrivateCAFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Oktober 2018, 16:54 UTC
- Waktu teredit: 23 Oktober 2018, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCertificateManagerPrivateCAPrivilegedUser

Deskripsi: Menyediakan akses pengguna sertifikat istimewa ke Otoritas AWS Sertifikat Pribadi Manajer Sertifikat

`AWSCertificateManagerPrivateCAPrivilegedUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCertificateManagerPrivateCAPrivilegedUser` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 Juni 2019, 17:43 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAPrivilegedUser`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/*CACertificate*/V*"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCertificateManagerPrivateCAReadOnly

Deskripsi: Menyediakan akses baca saja ke Otor AWS itas Sertifikat Pribadi Manajer Sertifikat

`AWSCertificateManagerPrivateCAReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCertificateManagerPrivateCAReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Oktober 2018, 16:57 UTC
- Waktu teredit: 17 Agustus 2020, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:DescribeCertificateAuthorityAuditReport",
      "acm-pca:ListCertificateAuthorities",
      "acm-pca:GetCertificateAuthorityCsr",
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:GetCertificate",
```

```
      "acm-pca:GetPolicy",
      "acm-pca:ListPermissions",
      "acm-pca:ListTags"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCertificateManagerPrivateCAUser

Deskripsi: Menyediakan akses pengguna sertifikat ke Otor AWS itas Sertifikat Pribadi Manajer Sertifikat

`AWSCertificateManagerPrivateCAUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCertificateManagerPrivateCAUser` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Oktober 2018, 16:53 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
```

```
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCertificateManagerReadOnly

Deskripsi: Menyediakan akses baca saja ke Manajer AWS Sertifikat (ACM).

`AWSCertificateManagerReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCertificateManagerReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Januari 2016, 17:07 UTC
- Waktu teredit: 13 Agustus 2026, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate",
      "acm:ListCertificates",
      "acm:SearchCertificates",
      "acm:GetCertificate",
      "acm:ListTagsForCertificate",
      "acm:GetAccountConfiguration",
      "acm:DescribeAcmeAccount",
      "acm:DescribeAcmeDomainValidation",
      "acm:DescribeAcmeEndpoint",
      "acm:DescribeAcmeExternalAccountBinding",
      "acm:ListAcmeAccounts",
      "acm:ListAcmeDomainValidations",
      "acm:ListAcmeEndpoints",
      "acm:ListAcmeExternalAccountBindings",
      "acm:ListTagsForResource",
      "acm:ListCertificateDomainValidations"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSChatbotServiceLinkedRolePolicy

Deskripsi: Peran Tertaut Layanan yang digunakan oleh AWS Chatbot.

`AWSChatbotServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 18 November 2019, 16:39 UTC
- Waktu teredit: 18 November 2019, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Unsubscribe",
```

```
        "sns:Subscribe",
        "sns:ListSubscriptions"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/chatbot/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCleanRoomsFullAccess

Deskripsi: Memungkinkan akses penuh ke sumber AWS daya Kamar Bersih dan akses ke yang terkait Layanan AWS.

`AWSCleanRoomsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCleanRoomsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Januari 2023, 16:10 UTC

- Waktu teredit: 21 Maret 2024, 15:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*"
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ConsolePickQueryResultsBucketListAll",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SetQueryResultsBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::cleanrooms-queryresults*"
    },
    {
      "Sid" : "WriteQueryResults",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::cleanrooms-queryresults*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleDisplayQueryResults",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::cleanrooms-queryresults*"
    },
    {
      "Sid" : "EstablishLogDeliveries",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCleanRoomsFullAccessNoQuerying

Deskripsi: Mengizinkan akses penuh AWS ke sumber daya Kamar Bersih kecuali untuk kueri dalam kolaborasi dan akses ke terkait Layanan AWS.

`AWSCleanRoomsFullAccessNoQueryingadalah` kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCleanRoomsFullAccessNoQuerying` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Januari 2023, 16:12 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:CreateAnalysisTemplate",
        "cleanrooms:CreateCollaboration",
        "cleanrooms:CreateConfiguredTable",
        "cleanrooms:CreateConfiguredTableAnalysisRule",
        "cleanrooms:CreateConfiguredTableAssociation",
        "cleanrooms:CreateMembership",
```

```
        "cleanrooms:DeleteAnalysisTemplate",
        "cleanrooms:DeleteCollaboration",
        "cleanrooms:DeleteConfiguredTable",
        "cleanrooms:DeleteConfiguredTableAnalysisRule",
        "cleanrooms:DeleteConfiguredTableAssociation",
        "cleanrooms:DeleteMember",
        "cleanrooms:DeleteMembership",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:UpdateAnalysisTemplate",
        "cleanrooms:UpdateCollaboration",
        "cleanrooms:UpdateConfiguredTable",
        "cleanrooms:UpdateConfiguredTableReference",
        "cleanrooms:UpdateConfiguredTableAllowedColumns",
        "cleanrooms:UpdateConfiguredTableAnalysisRule",
        "cleanrooms:UpdateConfiguredTableAssociation",
        "cleanrooms:UpdateMembership",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:UntagResource",
        "cleanrooms:TagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CleanRoomsNoQuerying",
      "Effect" : "Deny",
      "Action" : [
```

```
        "cleanrooms:StartProtectedQuery",
        "cleanrooms:UpdateProtectedQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*"
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EstablishLogDeliveries",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsDescribe",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
```

```
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCleanRoomsMLFullAccess

Deskripsi: Memungkinkan akses penuh ke AWS sumber daya ML Kamar Bersih dan akses ke yang terkait Layanan AWS.

`AWSCleanRoomsMLFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCleanRoomsMLFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2023, 21:02 UTC
- Waktu teredit: 12 Februari 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsMLFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms-ml:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/cleanrooms-ml*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms-ml.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CleanRoomsConsoleNavigation",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:GetCollaboration",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
```

```
        "cleanrooms:GetMembership",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CollaborationMembershipCheck",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:ListMembers"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cleanrooms-ml.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AssociateModels",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:CreateConfiguredAudienceModelAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagAssociations",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:TagResource"
      ],
```

```
      "Resource" : "arn:aws:cleanrooms:*:*:membership/*/
configuredaudiencemodelassociation/*"
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/cleanrooms-ml*",
        "arn:aws:iam::*:role/role/cleanrooms-ml*"
      ]
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanroomsml*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
```

```
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsolePickOutputBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsolePickS3Location",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*cleanrooms-ml*"
    },
    {
      "Sid" : "ConsoleDescribeECRRepositories",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeRepositories",
        "ecr:ListImages"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*"
    },
    {
      "Sid" : "PassCleanRoomsResources",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:PassMembership",
```

```
        "cleanrooms:PassCollaboration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCleanRoomsMLReadOnlyAccess

Deskripsi: Mengizinkan akses baca-saja ke sumber daya ML AWS Kamar Bersih dan akses baca-saja ke sumber daya Kamar Bersih terkait AWS

`AWSCleanRoomsMLReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCleanRoomsMLReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2023, 20:55 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsConsoleNavigation",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CleanRoomsMLRead",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms-ml:Get*",
        "cleanrooms-ml:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassCleanRoomsResources",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cleanrooms:PassMembership",
        "cleanrooms:PassCollaboration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCleanRoomsReadOnlyAccess

Deskripsi: Mengizinkan akses baca-saja ke sumber daya Kamar AWS Bersih dan akses baca-saja ke sumber daya AWS Glue dan Amazon Logs terkait. CloudWatch

`AWSCleanRoomsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCleanRoomsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Januari 2023, 16:10 UTC
- Waktu teredit: 12 Januari 2023, 16:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsRead",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:BatchGet*",
        "cleanrooms:Get*",
        "cleanrooms:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
```

```
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCleanRoomsServiceRolePolicy

Deskripsi: AWS Izinkan Kamar Bersih mengakses AWS layanan lain seperti CloudWatch API atas nama Anda.

`AWSCleanRoomsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 15 Desember 2025, 17:49 UTC
- Waktu teredit: 15 Desember 2025, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCleanRoomsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Clean Rooms"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCloud9Administrator

Deskripsi: Menyediakan akses administrator ke AWS Cloud9.

`AWSCloud9Administrator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloud9Administrator` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2017, 16:17 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9Administrator`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:*",
        "iam:GetUser",
        "iam:ListUsers",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:session/*"
      ]
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCloud9EnvironmentMember

Deskripsi: Menyediakan kemampuan untuk diundang ke lingkungan pengembangan bersama AWS Cloud9.

`AWSCloud9EnvironmentMember`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloud9EnvironmentMember` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2017, 16:18 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:GetUserSettings",
        "cloud9:UpdateUserSettings",
        "cloud9:GetMigrationExperiences",
        "iam:GetUser",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:DescribeEnvironmentMemberships"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true",
          "cloud9:EnvironmentId" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
        "StringEquals" : {
```

```
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:session/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCloud9ServiceRolePolicy

Deskripsi: Kebijakan Peran Terkait Layanan untuk AWS Cloud9

`AWSCloud9ServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 30 November 2017, 13:44 UTC
- Waktu teredit: 03 September 2026, 23:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "ec2:TerminateInstances",
```

```
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-cloud9-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : "aws-cloud9-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-name" : "aws-cloud9-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
```

```
        "ec2:StopInstances"
      ],
      "Resource" : [
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/cloud9/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSCloud9SSMAccessRole"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack"
          ]
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCloud9SSMInstanceProfile

Deskripsi: Kebijakan ini akan digunakan untuk melampirkan peran InstanceProfile yang akan memungkinkan Cloud9 menggunakan Manajer Sesi SSM untuk terhubung ke instance

`AWSCloud9SSMInstanceProfile`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloud9SSMInstanceProfile` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Mei 2020, 11:40 UTC
- Waktu teredit: 14 Mei 2020, 11:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCloud9User

Deskripsi: Memberikan izin untuk membuat lingkungan pengembangan AWS Cloud9 dan mengelola lingkungan yang dimiliki.

`AWSCloud9User`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloud9User` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2017, 16:16 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC

- ARN: `arn:aws:iam::aws:policy/AWSCloud9User`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:UpdateUserSettings",
        "cloud9:GetUserSettings",
        "cloud9:GetMigrationExperiences",
        "iam:GetUser",
        "iam:ListUsers",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:CreateEnvironmentEC2",
        "cloud9:CreateEnvironmentSSH"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "cloud9:OwnerArn" : "true"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:GetUserPublicKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:DescribeEnvironmentMemberships"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true",
          "cloud9:EnvironmentId" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
```

```
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:session/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCloudFormationFullAccess

Deskripsi: Menyediakan akses penuh ke AWS CloudFormation.

`AWSCloudFormationFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudFormationFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juli 2019, 21:50 UTC
- Waktu teredit: 26 Juli 2019, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCloudFormationReadOnlyAccess

Deskripsi: Menyediakan akses ke AWS CloudFormation melalui Konsol Manajemen AWS.

`AWSCloudFormationReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudFormationReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:Describe*",
        "cloudformation:BatchDescribe*",
        "cloudformation:EstimateTemplateCost",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "cloudformation:Detect*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCloudFrontLogger

Deskripsi: Memberikan izin CloudFront penulisan Logger ke CloudWatch Log.

`AWSCloudFrontLogger`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 12 Juni 2018, 20:15 UTC

- Waktu teredit: 22 November 2019, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCloudFrontVPCOriginServiceRolePolicy

Deskripsi: Memungkinkan CloudFront untuk mengelola Antarmuka Jaringan Elastis EC2 dan Grup Keamanan atas nama Anda.

`AWSCloudFrontVPCOriginServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 24 Oktober 2024, 17:45 UTC
- Waktu teredit: 24 Oktober 2024, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontVPCOriginServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Action1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws.cloudfront.vpcorigin" : "enabled"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
```

```
      "Sid" : "EC2Action2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "EC2Action3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws.cloudfront.vpcorigin" : "enabled"
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "EC2Action4",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "EC2Action5",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/aws.cloudfront.vpcorigin" : "enabled"
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action6",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action7",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws.cloudfront.vpcorigin" : "enabled",
          "ec2:CreateAction" : [
            "CreateNetworkInterface",
            "CreateSecurityGroup"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "ElbAction1",
      "Effect" : "Allow",
      "Action" : [
```

```
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCloudHSMFullAccess

Deskripsi: Menyediakan akses penuh ke semua sumber daya CloudHSM.

`AWSCloudHSMFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudHSMFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu teredit: 06 Februari 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudhsm:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCloudHSMReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke semua sumber daya CloudHSM.

`AWSCloudHSMReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudHSMReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu teredit: 06 Februari 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:Get*",
        "cloudhsm:List*",
        "cloudhsm:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCloudHSMRole

Deskripsi: Kebijakan default untuk peran layanan AWS CloudHSM.

`AWSCloudHSMRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudHSMRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 06 Februari 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateTags",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCloudMapDiscoverInstanceAccess

Deskripsi: Menyediakan akses ke API penemuan AWS Cloud Peta.

`AWSCloudMapDiscoverInstanceAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudMapDiscoverInstanceAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2018, 00:02 UTC
- Waktu teredit: 20 September 2023, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCloudMapFullAccess

Deskripsi: Menyediakan akses penuh ke semua tindakan AWS Cloud Peta.

`AWSCloudMapFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudMapFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 28 November 2018, 23:57 UTC
- Waktu teredit: 29 Juli 2020 19.15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "servicediscovery:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCloudMapReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke semua tindakan AWS Cloud Peta.

`AWSCloudMapReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudMapReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2018, 23:45 UTC
- Waktu teredit: 20 September 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCloudMapRegisterInstanceAccess

Deskripsi: Menyediakan akses tingkat pendaftar ke tindakan AWS Cloud Peta.

`AWSCloudMapRegisterInstanceAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudMapRegisterInstanceAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2018, 00:04 UTC
- Waktu teredit: 20 September 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:DeregisterInstance",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCloudShellFullAccess

Deskripsi: Hibah menggunakan AWS CloudShell dengan semua fitur

`AWSCloudShellFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudShellFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Desember 2020, 18:07 UTC
- Waktu teredit: 15 Desember 2020, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudShellFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudshell:*"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCloudTrail_FullAccess

Deskripsi: Menyediakan akses penuh ke AWS CloudTrail.

`AWSCloudTrail_FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudTrail_FullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Oktober 2020, 23:41 UTC
- Waktu teredit: 22 Februari 2021, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:AddPermission",
        "sns:CreateTopic",
        "sns:SetTopicAttributes",
        "sns:GetTopicAttributes"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:aws-cloudtrail-logs*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-cloudtrail-logs*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudtrail:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws-cloudtrail-logs*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetUser"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateKey",
        "kms:CreateAlias",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCloudTrail_ReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke AWS CloudTrail.

`AWSCloudTrail_ReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudTrail_ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 14 Juni 2022, 17:19 UTC
- Waktu teredit: 14 Juni 2022, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:Get*",
        "cloudtrail:Describe*",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

Deskripsi: Kebijakan ini digunakan oleh peran terkait layanan bernama AWSServiceRoleForCloudWatchAlarms _actionsSMincidents. CloudWatch menggunakan peran terkait layanan ini untuk melakukan tindakan Manajer Insiden AWS System Manager saat CloudWatch alarm masuk ke status ALARM. Kebijakan ini memberikan izin untuk memulai insiden atas nama Anda.

`AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 27 April 2021, 13:30 UTC
- Waktu teredit: 27 April 2021 13.30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-incidents:StartIncident",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCloudWatchOmniServiceRolePolicy

Deskripsi: Menye CloudWatch diakan akses Omni untuk mengelola sumber daya perekam AWS konfigurasi, konfigurasi telemetri, dan peran IAM pendukung untuk pengaktifan organisasi.

`AWSCloudWatchOmniServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 22 September 2026, 05:37 UTC
- Waktu teredit: 24 September 2026, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchOmniServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateManagedCloudWatchIntegration",
      "Effect" : "Allow",
      "Action" : "cloudwatch:CreateIntegration",
      "Resource" : "arn:aws:cloudwatch:*:*:integration/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOmniManaged"
        },
        "StringEquals" : {
          "aws:RequestTag/CloudWatchOmniManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagOperationForCloudWatchIntegration",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:TagResource"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:integration/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOmniManaged"
        },
        "StringEquals" : {
          "aws:RequestTag/CloudWatchOmniManaged" : "true",
          "aws:ResourceTag/CloudWatchOmniManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "ListCloudWatchIntegration",
      "Effect" : "Allow",
      "Action" : "cloudwatch:ListIntegrations",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DeleteManagedCloudWatchIntegration",
      "Effect" : "Allow",
      "Action" : "cloudwatch:DeleteIntegration",
      "Resource" : "arn:aws:cloudwatch:*:*:integration/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CloudWatchOmniManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageConfigServiceLinkedRecorder",
      "Effect" : "Allow",
      "Action" : [
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DescribeConfigurationRecorderStatus",
        "config:DeleteServiceLinkedConfigurationRecorder"
      ],
      "Resource" : "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForCloudWatch/*"
    },
    {
      "Sid" : "CreateConfigServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "CreateCloudWatchOmniAWSIntegrationRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/CloudWatchOmniAWSIntegrationRole-
*",
      "Condition" : {
        "ArnEquals" : {
          "iam:RoleTemplateARN" : "arn:aws:iam::aws:role-template/
cloudwatch.amazonaws.com/CloudWatchOmniAWSIntegrationForOrgRoleTemplate:1"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReadRoleTemplate",
      "Effect" : "Allow",
      "Action" : "iam:GetRoleTemplateVersion",
      "Resource" : "arn:aws:iam::aws:role-template/cloudwatch.amazonaws.com/
CloudWatchOmniAWSIntegrationForOrgRoleTemplate:1"
    },
    {
      "Sid" : "PassRolePermissionForCloudWatchOmniAWSIntegrationRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/CloudWatchOmniAWSIntegrationRole-
*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cloudwatch.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListIamUsersAndRoles",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetAwsAccountInformation",
      "Effect" : "Allow",
      "Action" : "account:GetAccountInformation",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetCloudWatchOmniAWSIntegrationRole",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/service-role/CloudWatchOmniAWSIntegrationRole-
*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodeArtifactAdminAccess

Deskripsi: Menyediakan akses penuh ke AWS CodeArtifact melalui Konsol Manajemen AWS.

`AWSCodeArtifactAdminAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeArtifactAdminAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 Juni 2020, 23:53 UTC
- Waktu teredit: 16 Juni 2020, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodeArtifactReadOnlyAccess

Deskripsi: Menyediakan akses baca saja AWS CodeArtifact melalui Konsol Manajemen AWS.

`AWSCodeArtifactReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeArtifactReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Juni 2020, 21:23 UTC
- Waktu teredit: 25 Juni 2020, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:Describe*",
        "codeartifact:Get*",
        "codeartifact:List*",
        "codeartifact:ReadFromRepository"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodeBuildAdminAccess

Deskripsi: Menyediakan akses penuh ke AWS CodeBuild melalui Konsol Manajemen AWS. Juga lampirkan AmazonS3ReadOnlyAccess untuk menyediakan akses untuk mengunduh artefak build, dan IAMFullAccess lampirkan untuk membuat dan mengelola peran layanan CodeBuild.

`AWSCodeBuildAdminAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeBuildAdminAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2016, 19:04 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess`

Versi kebijakan

Versi kebijakan: v20 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
```

```
        "codecommit:ListRepositories",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "elasticfilesystem:DescribeFileSystems",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CWLDeleteLogGroupAccess",
      "Action" : [
        "logs:DeleteLogGroup"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*:log-stream:*"
    },
    {
      "Sid" : "SSMParameterWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
    },
    {
      "Sid" : "SSMStartSessionAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
    },
    {
      "Sid" : "SSMOpenDataChannelAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    },
    {
      "Sid" : "CodeStarConnectionsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:CreateConnection",
        "codestar-connections:DeleteConnection",
        "codestar-connections:UpdateConnectionInstallation",
        "codestar-connections:TagResource",
        "codestar-connections:UntagResource",
        "codestar-connections:ListConnections",
        "codestar-connections:ListInstallationTargets",
        "codestar-connections:ListTagsForResource",
        "codestar-connections:GetConnection",
        "codestar-connections:GetIndividualAccessToken",
        "codestar-connections:GetInstallationUrl",
        "codestar-connections:PassConnection",
        "codestar-connections:StartOAuthHandshake",
        "codestar-connections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
```

```
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codebuild:*:*:project/*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodeBuildDeveloperAccess

Deskripsi: Menyediakan akses ke AWS CodeBuild melalui Konsol Manajemen AWS, tetapi tidak mengizinkan administrasi CodeBuild proyek. Juga lampirkan AmazonS3ReadOnlyAccess untuk memberikan akses untuk mengunduh artefak build.

`AWSCodeBuildDeveloperAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeBuildDeveloperAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2016, 19:02 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess`

Versi kebijakan

Versi kebijakan: v21 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:StartBuild",
        "codebuild:StopBuild",
        "codebuild:StartBuildBatch",
        "codebuild:StopBuildBatch",
        "codebuild:RetryBuild",
        "codebuild:RetryBuildBatch",
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codebuild:List*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMParameterWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter"
      ],
```

```
      "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
    },
    {
      "Sid" : "SSMStartSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
    },
    {
      "Sid" : "SSMOpenDataChannelAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    },
    {
      "Sid" : "CodeStarConnectionsUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
```

```
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codebuild:*:*:project/*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodeBuildReadOnlyAccess

Deskripsi: Menyediakan akses baca saja AWS CodeBuild melalui Konsol Manajemen AWS. Juga lampirkan AmazonS3ReadOnlyAccess untuk memberikan akses untuk mengunduh artefak build.

`AWSCodeBuildReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeBuildReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2016, 19:03 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:List*",
```

```
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codebuild:*:*:project/*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodeCommitFullAccess

Deskripsi: Menyediakan akses penuh ke AWS CodeCommit melalui Konsol Manajemen AWS.

`AWSCodeCommitFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeCommitFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Juli 2015, 17:02 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitFullAccess`

Versi kebijakan

Versi kebijakan: v13 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codecommit*"
    },
```

```
    {
      "Sid" : "SNSTopicAndSubscriptionReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccessKeys",
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMUserSSHKeys",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
```

```
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMSelfManageServiceSpecificCredentials",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codecommit:*:*:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:AssociateRepository",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DisassociateRepository",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodeCommitPowerUser

Deskripsi: Menyediakan akses penuh ke AWS CodeCommit repositori, tetapi tidak mengizinkan penghapusan repositori.

`AWSCodeCommitPowerUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeCommitPowerUser` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Juli 2015, 17:06 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitPowerUser`

Versi kebijakan

Versi kebijakan: v18 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:AssociateApprovalRuleTemplateWithRepository",
        "codecommit:BatchAssociateApprovalRuleTemplateWithRepositories",
        "codecommit:BatchDisassociateApprovalRuleTemplateFromRepositories",
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
        "codecommit:Create*",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:Describe*",
        "codecommit:DisassociateApprovalRuleTemplateFromRepository",
        "codecommit:EvaluatePullRequestApprovalRules",
```

```
        "codecommit:Get*",
        "codecommit:List*",
        "codecommit:Merge*",
        "codecommit:OverridePullRequestApprovalRules",
        "codecommit:Put*",
        "codecommit:Post*",
        "codecommit:TagResource",
        "codecommit:Test*",
        "codecommit:UntagResource",
        "codecommit:Update*",
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
```

```
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccessKeys",
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMUserSSHKeys",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
```

```
      "Sid" : "IAMSelfManageServiceSpecificCredentials",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codecommit:*:*:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:AssociateRepository",
```

```
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DisassociateRepository",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodeCommitReadOnly

Deskripsi: Menyediakan akses baca saja AWS CodeCommit melalui Konsol Manajemen AWS.

`AWSCodeCommitReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeCommitReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Juli 2015, 17:05 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitReadOnly`

Versi kebijakan

Versi kebijakan: v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
        "codecommit:Describe*",
        "codecommit:EvaluatePullRequestApprovalRules",
        "codecommit:Get*",
        "codecommit:List*",
        "codecommit:GitPull"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials",
        "iam:ListAccessKeys",
        "iam:GetSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "CodeStarNotificationsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codecommit:*:*:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodeDeployDeployerAccess

Deskripsi: Menyediakan akses untuk mendaftar dan menerapkan revisi.

`AWSCodeDeployDeployerAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeDeployDeployerAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Mei 2015, 18:18 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codedeploy:Batch*",
        "codedeploy:CreateDeployment",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codedeploy:RegisterApplicationRevision"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codedeploy:*:*:application:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodeDeployFullAccess

Deskripsi: Menyediakan akses penuh ke CodeDeploy sumber daya.

`AWSCodeDeployFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeDeployFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Mei 2015, 18:13 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "codedeploy:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codedeploy:*:*:application:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodeDeployReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke CodeDeploy sumber daya.

`AWSCodeDeployReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeDeployReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Mei 2015, 18:21 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codedeploy:*:*:application:*"
```

```
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodeDeployRole

Deskripsi: Menye CodeDeploy diakan akses layanan untuk memperluas tag dan berinteraksi dengan Auto Scaling atas nama Anda.

`AWSCodeDeployRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeDeployRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 04 Mei 2015, 18:05 UTC

- Waktu teredit: 10 September 2026, 10:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:DeleteLifecycleHook",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:PutLifecycleHook",
        "autoscaling:RecordLifecycleActionHeartbeat",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:EnableMetricsCollection",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:SuspendProcesses",
        "autoscaling:ResumeProcesses",
        "autoscaling:AttachLoadBalancers",
        "autoscaling:AttachLoadBalancerTargetGroups",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutWarmPool",
```

```
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DeleteAutoScalingGroup",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:TerminateInstances",
        "tag:GetResources",
        "sns:Publish",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodeDeployRoleForCloudFormation

Deskripsi: Menye CodeDeploy diakan akses layanan untuk memanggil fungsi Lambda atas nama Anda untuk melakukan blue/green penerapan melalui. CloudFormation

`AWSCodeDeployRoleForCloudFormation`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeDeployRoleForCloudFormation` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Mei 2020, 17:12 UTC
- Waktu teredit: 19 Mei 2020, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodeDeployRoleForECS

Deskripsi: Menye CodeDeploy diakan akses luas layanan untuk melakukan penerapan ECS blue/green atas nama Anda. Memberikan akses penuh ke layanan dukungan, seperti akses penuh untuk membaca semua objek S3, memanggil semua fungsi Lambda, menerbitkan ke semua topik SNS dalam akun dan memperbarui semua layanan ECS.

`AWSCodeDeployRoleForECS`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeDeployRoleForECS` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2018, 20:40 UTC
- Waktu teredit: 23 September 2019, 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Action" : [
        "ecs:DescribeServices",
        "ecs:CreateTaskSet",
        "ecs:UpdateServicePrimaryTaskSet",
        "ecs:DeleteTaskSet",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:ModifyRule",
        "lambda:InvokeFunction",
        "cloudwatch:DescribeAlarms",
        "sns:Publish",
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ecs-tasks.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodeDeployRoleForECSLimited

Deskripsi: Menye CodeDeploy diakan akses terbatas layanan untuk melakukan penerapan ECS blue/green atas nama Anda.

`AWSCodeDeployRoleForECSLimited`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeDeployRoleForECSLimited` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2018, 20:42 UTC
- Waktu teredit: 23 September 2019, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ecs:DescribeServices",
        "ecs:CreateTaskSet",
        "ecs:UpdateServicePrimaryTaskSet",
        "ecs:DeleteTaskSet",
        "cloudwatch:DescribeAlarms"
      ],
```

```
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:CodeDeployTopic_*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:ModifyRule"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      },
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsTaskExecutionRole",
        "arn:aws:iam::*:role/ECSTaskExecution*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ecs-tasks.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodeDeployRoleForLambda

Deskripsi: Menye CodeDeploy diakan akses layanan untuk melakukan penerapan Lambda atas nama Anda.

`AWSCodeDeployRoleForLambda`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeDeployRoleForLambda` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 28 November 2017, 14:05 UTC

- Waktu teredit: 03 Desember 2019, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "lambda:UpdateAlias",
        "lambda:GetAlias",
        "lambda:GetProvisionedConcurrencyConfig",
        "sns:Publish"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/CodeDeploy/*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      },
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodeDeployRoleForLambdaLimited

Deskripsi: Menye CodeDeploy diakan akses terbatas layanan untuk melakukan penerapan Lambda atas nama Anda.

`AWSCodeDeployRoleForLambdaLimited`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeDeployRoleForLambdaLimited` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 17 Agustus 2020, 17:14 UTC

- Waktu teredit: 17 Agustus 2020, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "lambda:UpdateAlias",
        "lambda:GetAlias",
        "lambda:GetProvisionedConcurrencyConfig"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/CodeDeploy/*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      },
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodePipeline_FullAccess

Deskripsi: Menyediakan akses penuh ke AWS CodePipeline melalui Konsol Manajemen AWS.

`AWSCodePipeline_FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodePipeline_FullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Agustus 2020, 22:38 UTC
- Waktu teredit: 14 Maret 2024, 17:06 UTC

- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudformation:ListChangeSets",
        "cloudtrail:DescribeTrails",
        "codebuild:BatchGetProjects",
        "codebuild:CreateProject",
        "codebuild:ListCuratedEnvironmentImages",
        "codebuild:ListProjects",
        "codecommit:ListBranches",
        "codecommit:GetReferences",
        "codecommit:ListRepositories",
        "codedeploy:BatchGetDeploymentGroups",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:ListClusters",
        "ecs:ListServices",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeEnvironments",
        "iam:ListRoles",
        "iam:GetRole",
```

```
        "lambda:ListFunctions",
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:DescribeRule",
        "opsworks:DescribeApps",
        "opsworks:DescribeLayers",
        "opsworks:DescribeStacks",
        "s3:ListAllMyBuckets",
        "sns:ListTopics",
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes",
        "states:ListStateMachines"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "CodePipelineAuthoringAccess"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketPolicy",
        "s3:GetBucketVersioning",
        "s3:GetObjectVersion",
        "s3:CreateBucket",
        "s3:PutBucketPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3::*:codepipeline-*",
      "Sid" : "CodePipelineArtifactsReadWriteAccess"
    },
    {
      "Action" : [
        "cloudtrail:PutEventSelectors",
        "cloudtrail:CreateTrail",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:StartLogging"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudtrail:*:*:trail/codepipeline-source-trail",
      "Sid" : "CodePipelineSourceTrailReadWriteAccess"
    },
```

```
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/cwe-role-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "events.amazonaws.com"
          ]
        }
      },
      "Sid" : "EventsIAMPassRole"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "codepipeline.amazonaws.com"
          ]
        }
      },
      "Sid" : "CodePipelineIAMPassRole"
    },
    {
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:DisableRule",
        "events:RemoveTargets"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:events:*:*:rule/codepipeline-*"
      ],
```

```
      "Sid" : "CodePipelineEventsReadWriteAccess"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codepipeline:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodePipeline_ReadOnlyAccess

Deskripsi: Menyediakan akses baca saja AWS CodePipeline melalui Konsol Manajemen AWS.

`AWSCodePipeline_ReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodePipeline_ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Agustus 2020, 22:25 UTC
- Waktu teredit: 03 Agustus 2020, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Statement" : [
```

```
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListActionExecutions",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "s3:ListAllMyBuckets",
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3::*:codepipeline-*"
    },
    {
      "Sid" : "CodeStarNotificationsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codepipeline:*"
        }
      }
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodePipelineApproverAccess

Deskripsi: Menyediakan akses untuk melihat dan menyetujui perubahan manual untuk semua pipeline

`AWSCodePipelineApproverAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodePipelineApproverAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Juli 2016, 18:59 UTC
- Waktu teredit: 02 Agustus 2017, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:PutApprovalResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodePipelineCustomActionAccess

Deskripsi: Menyediakan akses untuk tindakan kustom untuk jajak pendapat untuk detail pekerjaan (termasuk kredenSIAL sementara) dan melaporkan pembaruan status ke AWS CodePipeline.

`AWSCodePipelineCustomActionAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodePipelineCustomActionAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 09 Juli 2015, 17:02 UTC
- Waktu teredit: 09 Juli 2015, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
        "codepipeline:PutJobSuccessResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodeStarFullAccess

Deskripsi: Menyediakan akses penuh ke AWS CodeStar melalui Konsol Manajemen AWS.

`AWSCodeStarFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeStarFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 April 2017, 16:23 UTC
- Waktu teredit: 28 Maret 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeStarFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeStarEC2",
      "Effect" : "Allow",
      "Action" : [
        "codestar:*",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "cloud9:DescribeEnvironment*",
        "cloud9:ValidateEnvironmentName"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarCF",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*",
        "cloudformation:ListStacks*",
        "cloudformation:GetTemplateSummary"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awscodestar-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodeStarNotificationsServiceRolePolicy

Deskripsi: Mengiz AWS CodeStar inkan Pemberitahuan mengakses CloudWatch Acara Amazon atas nama Anda

`AWSCodeStarNotificationsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran

- Waktu pembuatan: 05 November 2019, 16:10 UTC
- Waktu teredit: 19 Maret 2020, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "events:PutTargets",
        "events:PutRule",
        "events:DescribeRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/awscodestarnotifications-*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "sns:CreateTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:CodeStarNotifications-*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommentsForComparedCommit",
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:UpdateSlackChannelConfiguration",
        "codecommit:GetDifferences",
```

```
        "codepipeline:ListActionExecutions"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "codecommit:GetFile"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/ExcludeFileContentFromNotifications" : "true"
        }
      },
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCodeStarServiceRole

Deskripsi: JANGAN GUNAKAN - Kebijakan Peran AWS CodeStar Layanan yang memberikan hak administratif CodeStar untuk mengelola IAM dan sumber daya layanan lainnya atas nama pelanggan.

`AWSCodeStarServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodeStarServiceRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 April 2017, 15:20 UTC

- Waktu teredit: 08 September 2026, 12:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProjectEventRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:RemoveTargets",
        "events:PutRule",
        "events:DeleteRule",
        "events:DescribeRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/awscodestar-*"
      ]
    },
    {
      "Sid" : "ProjectStack",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*Stack*",
        "cloudformation:CreateChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:GetTemplate"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awscodestar-*",
```

```
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/aws-cloud9-*",
        "arn:aws:cloudformation:*:aws:transform/CodeStar*"
      ]
    },
    {
      "Sid" : "ProjectStackTemplate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "cloudformation:DescribeChangeSet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awscodestar-*",
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/aws-cloud9-*",
        "arn:aws:cloudformation:*:aws:transform/CodeStar*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack",
            "UpdateStack",
            "CreateChangeSet",
            "ExecuteChangeSet"
          ]
        }
      }
    },
    {
      "Sid" : "ProjectQuickstarts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::awscodestar-*/*"
      ]
    },
    {
      "Sid" : "ProjectS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:*"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-codestar-*",
        "arn:aws:s3:::elasticbeanstalk-*"
      ]
    },
    {
      "Sid" : "ProjectServices",
      "Effect" : "Allow",
      "Action" : [
        "codestar:*",
        "codecommit:*",
        "codepipeline:*",
        "codedeploy:*",
        "codebuild:*",
        "autoscaling:*",
        "cloudwatch:Put*",
        "ec2:*",
        "elasticbeanstalk:*",
        "elasticloadbalancing:*",
        "iam:ListRoles",
        "logs:*",
        "sns:*",
        "cloud9:CreateEnvironmentEC2",
        "cloud9:DeleteEnvironment",
        "cloud9:DescribeEnvironment*",
        "cloud9:ListEnvironments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ProjectWorkerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
```

```
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:GetRole",
        "iam:PassRole",
        "iam:GetRolePolicy",
        "iam:PutRolePolicy",
        "iam:SetDefaultPolicyVersion",
        "iam:CreatePolicy",
        "iam:DeletePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CodeStarWorker*",
        "arn:aws:iam::*:policy/CodeStarWorker*",
        "arn:aws:iam::*:instance-profile/awscodestar-*"
      ]
    },
    {
      "Sid" : "ProjectTeamMembers",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachUserPolicy",
        "iam:DetachUserPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyArn" : [
            "arn:aws:iam::*:policy/CodeStar_*"
          ]
        }
      }
    },
    {
      "Sid" : "ProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreatePolicy",
        "iam:DeletePolicy",
```

```
        "iam:CreatePolicyVersion",
        "iam:DeletePolicyVersion",
        "iam:ListEntitiesForPolicy",
        "iam:ListPolicyVersions",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/CodeStar_*"
      ]
    },
    {
      "Sid" : "InspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-codestar-service-role",
        "arn:aws:iam::*:role/service-role/aws-codestar-service-role"
      ]
    },
    {
      "Sid" : "IAMLinkRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DescribeConfigRuleForARN",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigRules"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "ProjectCodeStarConnections",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ProjectCodeStarConnectionsPassConnections",
      "Effect" : "Allow",
      "Action" : "codestar-connections:PassConnection",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCompromisedKeyQuarantine

Deskripsi: Menolak akses ke tindakan tertentu, diterapkan oleh AWS tim jika kredentif pengguna IAM telah dikompromikan atau diekspos secara publik. Jangan hapus kebijakan ini. Sebagai gantinya, silakan ikuti instruksi yang ditentukan dalam email yang dikirimkan kepada Anda mengenai acara ini.

`AWSCompromisedKeyQuarantine`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCompromisedKeyQuarantine` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Agustus 2020, 18:04 UTC
- Waktu teredit: 11 Agustus 2020, 18:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
```

```
        "iam:UpdateAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateUser",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
        "lambda:CreateFunction",
        "lightsail:Create*",
        "lightsail:Start*",
        "lightsail:Delete*",
        "lightsail:Update*",
        "lightsail:GetInstanceAccessDetails",
        "lightsail:DownloadDefaultKeyPair"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCompromisedKeyQuarantineV2

Deskripsi: Menolak akses ke tindakan tertentu, diterapkan oleh AWS tim jika kredentif pengguna IAM telah dikompromikan atau diekspos secara publik. Jangan hapus kebijakan ini. Sebagai gantinya, ikuti instruksi yang ditentukan dalam kasus dukungan yang dibuat untuk Anda mengenai acara ini.

`AWSCompromisedKeyQuarantineV2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCompromisedKeyQuarantineV2` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 April 2021, 22:30 UTC
- Waktu teredit: 02 Oktober 2024, 16:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "cloudtrail:LookupEvents",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "iam:AddUserToGroup",
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
```

```
        "iam:CreatePolicyVersion",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PassRole",
        "iam:PutGroupPolicy",
        "iam:PutRolePolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:SetDefaultPolicyVersion",
        "iam:UpdateAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateLoginProfile",
        "iam:UpdateUser",
        "lambda:AddLayerVersionPermission",
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetPolicy",
        "lambda:ListTags",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lightsail:Create*",
        "lightsail:Delete*",
        "lightsail:DownloadDefaultKeyPair",
        "lightsail:GetInstanceAccessDetails",
        "lightsail:Start*",
        "lightsail:Update*",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketAcl",
        "s3:PutBucketOwnershipControls",
        "s3:DeleteBucketPolicy",
        "s3:ObjectOwnerOverrideToBucketOwner",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:ListAllMyBuckets",
```

```
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:AcceptReservedInstancesExchangeQuote",
        "ec2:CreateReservedInstancesListing",
        "savingsplans:CreateSavingsPlan",
        "ecs:CreateService",
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition",
        "ecr:GetAuthorizationToken",
        "bedrock:CreateModelInvocationJob",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:CreateFoundationModelAgreement",
        "bedrock:PutFoundationModelEntitlement",
        "bedrock:InvokeModel",
        "s3:CreateBucket",
        "s3:PutBucketCors",
        "s3:GetObject",
        "s3:ListBucket",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateProcessingJob",
        "ses:GetSendQuota",
        "ses:ListIdentities",
        "sts:GetSessionToken",
        "sts:GetFederationToken",
        "amplify:CreateDeployment",
        "amplify:CreateBackendEnvironment",
        "codebuild:CreateProject",
        "glue:CreateJob",
        "iam:DeleteRole",
        "iam:DeleteAccessKey",
        "iam:ListUsers",
        "lambda:GetEventSourceMapping",
        "sns:GetSMSAttributes",
        "mediapackagev2:CreateChannel"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCompromisedKeyQuarantineV3

Deskripsi: Menolak akses ke tindakan tertentu, diterapkan jika AWS kredentif pengguna IAM telah dikompromikan atau diekspos secara publik. Kebijakan ini bertujuan untuk membatasi potensi kerusakan yang mungkin disebabkan oleh aktivitas terkait penipuan yang menyebabkan tagihan tidak sah, sementara tidak berdampak pada sumber daya yang ada. Jangan hapus kebijakan ini. Sebagai gantinya, ikuti instruksi yang ditentukan dalam kasus dukungan yang dibuat untuk Anda mengenai acara ini.

`AWSCompromisedKeyQuarantineV3`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCompromisedKeyQuarantineV3` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Agustus 2024, 17:36 UTC
- Waktu teredit: 16 Maret 2026, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV3`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "cloudtrail:LookupEvents",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:AcceptReservedInstancesExchangeQuote",
        "ec2:CreateReservedInstancesListing",
        "iam:AddUserToGroup",
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreatePolicyVersion",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PassRole",
        "iam:PutGroupPolicy",
        "iam:PutRolePolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:SetDefaultPolicyVersion",
        "iam:UpdateAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateLoginProfile",
        "iam:UpdateUser",
        "iam:DeleteRole",
        "iam:DeleteAccessKey",
        "iam:ListUsers",
        "lambda:AddLayerVersionPermission",
        "lambda:AddPermission",
```

```
        "lambda:CreateFunction",
        "lambda:GetPolicy",
        "lambda:ListTags",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lambda:GetEventSourceMapping",
        "lightsail:Create*",
        "lightsail:Delete*",
        "lightsail:DownloadDefaultKeyPair",
        "lightsail:GetInstanceAccessDetails",
        "lightsail:Start*",
        "lightsail:Update*",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
        "organizations:LeaveOrganization",
        "organizations:AcceptHandshake",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketAcl",
        "s3:PutBucketOwnershipControls",
        "s3:DeleteBucketPolicy",
        "s3:ObjectOwnerOverrideToBucketOwner",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:ListAllMyBuckets",
        "s3:CreateBucket",
        "s3:PutBucketCors",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutEncryptionConfiguration",
        "savingsplans:CreateSavingsPlan",
        "ecs:CreateService",
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition",
        "ecr:GetAuthorizationToken",
        "bedrock:CreateModelInvocationJob",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:CreateFoundationModelAgreement",
        "bedrock:PutFoundationModelEntitlement",
```

```
        "bedrock:InvokeModel",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateProcessingJob",
        "ses:GetSendQuota",
        "ses:ListIdentities",
        "sts:GetSessionToken",
        "sts:GetFederationToken",
        "amplify:CreateDeployment",
        "amplify:CreateBackendEnvironment",
        "codebuild:CreateProject",
        "glue:CreateJob",
        "sns:GetSMSAttributes",
        "mediapackagev2:CreateChannel",
        "logs:PutLogEvents",
        "kms:PutKeyPolicy",
        "kms:RetireGrant",
        "kms:RevokeGrant",
        "kms:ScheduleKeyDeletion",
        "kms:DeleteImportedKeyMaterial"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:ViaService" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSConfigMultiAccountSetupPolicy

Deskripsi: Mengizinkan Config memanggil AWS layanan dan menyebarkan sumber daya konfigurasi di seluruh organisasi

`AWSConfigMultiAccountSetupPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 17 Juni 2019, 18:03 UTC
- Waktu teredit: 24 Februari 2023, 01:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "config:PutConfigRule",
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/config-
multiaccountsetup.amazonaws.com/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConformancePack",
        "config:DeleteConformancePack"
      ],
      "Resource" : "arn:aws:config:*:*:conformance-pack/aws-service-conformance-pack/
config-multiaccountsetup.amazonaws.com/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConformancePackStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "config-conforms.amazonaws.com"
        }
      }
    },
    {
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSConfigRemediationServiceRolePolicy

Deskripsi: Mengizinkan AWS Config memperbaiki sumber daya yang tidak sesuai atas nama Anda.

`AWSConfigRemediationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 18 Juni 2019, 21:21 UTC
- Waktu teredit: 18 Juni 2019, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
```

```
      },
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSConfigRoleForOrganizations

Deskripsi: Mengizinkan AWS Config memanggil API Organisasi yang hanya dapat dibaca AWS

`AWSConfigRoleForOrganizations`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSConfigRoleForOrganizations` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Maret 2018, 22:53 UTC
- Waktu teredit: 24 November 2020, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSConfigRulesExecutionRole

Deskripsi: Mengiz AWS inkan fungsi Lambda mengakses AWS Config API dan snapshot konfigurasi yang dikirimkan AWS Config secara berkala ke Amazon S3. Akses ini diperlukan oleh fungsi yang mengevaluasi perubahan konfigurasi untuk aturan konfigurasi kustom.

`AWSConfigRulesExecutionRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSConfigRulesExecutionRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 25 Maret 2016, 17:59 UTC
- Waktu teredit: 13 Mei 2019, 21:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/AWSLogs/*/Config/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:Put*",
        "config:Get*",
        "config:List*",
        "config:Describe*",
        "config:BatchGet*",
        "config:Select*"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSConfigServiceRolePolicy

Deskripsi: Mengizinkan Config memang AWS gil layanan dan mengumpulkan konfigurasi sumber daya atas nama Anda.

`AWSConfigServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 30 Mei 2018, 23:31 UTC
- Waktu teredit: 23 September 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v96 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigServiceRolePolicyStatementID1",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "access-analyzer:ValidatePolicy",
        "account-access:GetEntitlement",
        "account-access:ListEntitlements",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListTagsForResource",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListForms",
        "amplifyuibuilder:ListThemes",
        "aoss:BatchGetCollection",
```

```
        "aoss:BatchGetCollectionGroup",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollectionGroups",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListTagsForResource",
        "aoss:ListVpcEndpoints",
        "app-integrations:GetApplication",
        "app-integrations:GetDataIntegration",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListApplications",
        "app-integrations:ListDataIntegrations",
        "app-integrations:ListEventIntegrationAssociations",
        "app-integrations:ListEventIntegrations",
        "app-integrations:ListTagsForResource",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExperimentDefinition",
        "appconfig:GetExtension",
        "appconfig:GetExtensionAssociation",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExperimentDefinitions",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListExtensions",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlow",
        "appflow:ListFlows",
```

```
        "appflow:ListTagsForResource",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServices",
        "application-signals:ListTagsForResource",
        "applicationinsights:DescribeApplication",
        "applicationinsights:DescribeComponent",
        "applicationinsights:DescribeLogPattern",
        "applicationinsights:ListApplications",
        "applicationinsights:ListComponents",
        "applicationinsights:ListLogPatterns",
        "applicationinsights:ListLogPatternSets",
        "applicationinsights:ListTagsForResource",
        "appmesh:DescribeGatewayRoute",
        "appmesh:DescribeMesh",
        "appmesh:DescribeRoute",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:DescribeVirtualRouter",
        "appmesh:DescribeVirtualService",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListTagsForResource",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appstream:DescribeAppBlockBuilders",
```

```
        "appstream:DescribeAppBlocks",
        "appstream:DescribeApplications",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeFleets",
        "appstream:DescribeImageBuilders",
        "appstream:DescribeStacks",
        "appstream:ListAssociatedFleets",
        "appstream:ListAssociatedStacks",
        "appstream:ListTagsForResource",
        "appsync:GetApi",
        "appsync:GetApiAssociation",
        "appsync:GetApiCache",
        "appsync:GetChannelNamespace",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
        "appsync:GetGraphqlApi",
        "appsync:GetResolver",
        "appsync:GetSourceApiAssociation",
        "appsync:ListApis",
        "appsync:ListChannelNamespaces",
        "appsync:ListDataSources",
        "appsync:ListDomainNames",
        "appsync:ListGraphqlApis",
        "appsync:ListResolvers",
        "appsync:ListSourceApiAssociations",
        "appsync:ListTagsForResource",
        "appsync:ListTypes",
        "apptest:GetTestCase",
        "apptest:ListTagsForResource",
        "apptest:ListTestCases",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeAnomalyDetector",
        "aps:DescribeLoggingConfiguration",
        "aps:DescribeQueryLoggingConfiguration",
        "aps:DescribeResourcePolicy",
        "aps:DescribeRuleGroupsNamespace",
        "aps:DescribeScraper",
        "aps:DescribeScraperLoggingConfiguration",
        "aps:DescribeWorkspace",
        "aps:DescribeWorkspaceConfiguration",
        "aps:ListAnomalyDetectors",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListScrapers",
        "aps:ListTagsForResource",
```

```
        "aps:ListWorkspaces",
        "arc-region-switch:GetPlan",
        "arc-region-switch:ListPlans",
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListTagsForResource",
        "arc-zonal-shift:GetAutoshiftObserverNotificationStatus",
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListDataCatalogs",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:GetAssessmentFramework",
        "auditmanager:GetControl",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessments",
        "auditmanager:ListControls",
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "b2bi:GetCapability",
        "b2bi:GetPartnership",
        "b2bi:GetProfile",
        "b2bi:GetTransformer",
        "b2bi:ListCapabilities",
        "b2bi:ListPartnerships",
        "b2bi:ListProfiles",
        "b2bi:ListTagsForResource",
        "b2bi:ListTransformers",
        "backup-gateway:GetHypervisor",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:DescribeBackupVault",
```

```
        "backup:DescribeFramework",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeReportPlan",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:GetTieringConfiguration",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListFrameworks",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListReportPlans",
        "backup:ListRestoreTestingPlans",
        "backup:ListRestoreTestingSelections",
        "backup:ListTags",
        "backup:ListTieringConfigurations",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeConsumableResource",
        "batch:DescribeJobDefinitions",
        "batch:DescribeJobQueues",
        "batch:DescribeQuotaShare",
        "batch:DescribeSchedulingPolicies",
        "batch:DescribeServiceEnvironments",
        "batch:ListConsumableResources",
        "batch:ListQuotaShares",
        "batch:ListSchedulingPolicies",
        "batch:ListTagsForResource",
        "bcm-dashboards:GetDashboard",
        "bcm-dashboards:ListDashboards",
        "bcm-dashboards:ListTagsForResource",
        "bcm-data-exports:GetExport",
        "bcm-data-exports:ListExports",
        "bcm-data-exports:ListTagsForResource",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetApiKeyCredentialProvider",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetBrowserProfile",
        "bedrock-agentcore:GetCodeInterpreter",
```

```
        "bedrock-agentcore:GetConfigurationBundle",
        "bedrock-agentcore:GetEvaluator",
        "bedrock-agentcore:GetGateway",
        "bedrock-agentcore:GetGatewayTarget",
        "bedrock-agentcore:GetMemory",
        "bedrock-agentcore:GetOauth2CredentialProvider",
        "bedrock-agentcore:GetOnlineEvaluationConfig",
        "bedrock-agentcore:GetPaymentConnector",
        "bedrock-agentcore:GetPaymentCredentialProvider",
        "bedrock-agentcore:GetPaymentManager",
        "bedrock-agentcore:GetPolicy",
        "bedrock-agentcore:GetPolicyEngine",
        "bedrock-agentcore:GetPolicyEngineSummary",
        "bedrock-agentcore:GetPolicyGeneration",
        "bedrock-agentcore:GetPolicyGenerationSummary",
        "bedrock-agentcore:GetPolicySummary",
        "bedrock-agentcore:GetResourcePolicy",
        "bedrock-agentcore:GetTokenVault",
        "bedrock-agentcore:GetWorkloadIdentity",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListApiKeyCredentialProviders",
        "bedrock-agentcore:ListBrowserProfiles",
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListConfigurationBundles",
        "bedrock-agentcore:ListEvaluators",
        "bedrock-agentcore:ListGateways",
        "bedrock-agentcore:ListGatewayTargets",
        "bedrock-agentcore:ListMemories",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "bedrock-agentcore:ListOnlineEvaluationConfigs",
        "bedrock-agentcore:ListPaymentConnectors",
        "bedrock-agentcore:ListPaymentCredentialProviders",
        "bedrock-agentcore:ListPaymentManagers",
        "bedrock-agentcore:ListPolicies",
        "bedrock-agentcore:ListPolicyEngines",
        "bedrock-agentcore:ListPolicyEngineSummaries",
        "bedrock-agentcore:ListPolicyGenerations",
        "bedrock-agentcore:ListPolicyGenerationSummaries",
        "bedrock-agentcore:ListPolicySummaries",
        "bedrock-agentcore:ListTagsForResource",
        "bedrock-agentcore:ListWorkloadIdentities",
        "bedrock:GetAgent",
```

```
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAutomatedReasoningPolicy",
        "bedrock:GetBlueprint",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataSource",
        "bedrock:GetEvaluationJob",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetFoundationModel",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetPromptRouter",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListAutomatedReasoningPolicies",
        "bedrock:ListBlueprints",
        "bedrock:ListDataAutomationProjects",
        "bedrock:ListDataSources",
        "bedrock:ListEnforcedGuardrailsConfiguration",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlows",
        "bedrock:ListFlowVersions",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListPromptRouters",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "billing:GetBillingView",
        "billing:ListBillingViews",
        "billing:ListSourceViewsForBillingView",
        "billing:ListTagsForResource",
        "billingconductor:ListAccountAssociations",
```

```
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListTagsForResource",
        "braket:ListTagsForResource",
        "braket:SearchSpendingLimits",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ViewBudget",
        "cases:BatchGetCaseRule",
        "cases:BatchGetField",
        "cases:GetDomain",
        "cases:GetLayout",
        "cases:GetTemplate",
        "cases:ListCaseRules",
        "cases:ListDomains",
        "cases:ListFields",
        "cases:ListLayouts",
        "cases:ListTemplates",
        "cassandra:Select",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "chime:DescribeAppInstance",
        "chime:DescribeAppInstanceBot",
        "chime:DescribeAppInstanceUser",
        "chime:DescribeChannelFlow",
        "chime:ListAppInstanceBots",
        "chime:ListAppInstances",
        "chime:ListChannelFlows",
        "chime:ListTagsForResource",
        "cleanrooms-ml:GetConfiguredModelAlgorithm",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListConfiguredModelAlgorithms",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetConfiguredTable",
```

```
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListTagsForResource",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribePublisher",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:ListChangeSets",
        "cloudformation:ListResources",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
        "cloudformation:ListTypes",
        "cloudfront:DescribeFunction",
        "cloudfront:DescribeKeyValueStore",
        "cloudfront:GetAnycastIpList",
        "cloudfront:GetCachePolicy",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetConnectionGroup",
        "cloudfront:GetContinuousDeploymentPolicy",
        "cloudfront:GetDistributionTenant",
        "cloudfront:GetFunction",
```

```
        "cloudfront:GetKeyGroup",
        "cloudfront:GetMonitoringSubscription",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetOriginRequestPolicy",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:GetVpcOrigin",
        "cloudfront:ListAnycastIpLists",
        "cloudfront:ListCachePolicies",
        "cloudfront:ListCloudFrontOriginAccessIdentities",
        "cloudfront:ListConnectionGroups",
        "cloudfront:ListContinuousDeploymentPolicies",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListFunctions",
        "cloudfront:ListKeyGroups",
        "cloudfront:ListKeyValueStores",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListOriginRequestPolicies",
        "cloudfront:ListPublicKeys",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudfront:ListVpcOrigins",
        "cloudtrail:DescribeTrails",
        "cloudTrail:GetChannel",
        "cloudtrail:GetDashboard",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetResourcePolicy",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudTrail:ListChannels",
        "cloudtrail:ListDashboards",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:DescribeInsightRules",
```

```
        "cloudwatch:GetAlarmMuteRule",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListAlarmMuteRules",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListManagedInsightRules",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackageGroup",
        "codeartifact:DescribeRepository",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListAllowedRepositoriesForGroup",
        "codeartifact:ListDomains",
        "codeartifact:ListPackageGroups",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetFleets",
        "codebuild:BatchGetReportGroups",
        "codebuild:ListFleets",
        "codebuild:ListReportGroups",
        "codebuild:ListSourceCredentials",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListRepositories",
        "codecommit:ListTagsForResource",
        "codeconnections:GetConnection",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codedeploy:GetDeploymentConfig",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
```

```
        "codepipeline:ListWebhooks",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:ListConnections",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListTagsForResource",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:AdminGetUser",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeManagedLoginBranding",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeTerms",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetLogDeliveryConfiguration",
        "cognito-idp:GetUICustomization",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListTerms",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "comprehend:DescribeFlywheel",
        "comprehend:ListFlywheels",
        "comprehend:ListTagsForResource",
        "config:BatchGet*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:Put*",
        "config:Select*",
        "connect-campaigns:DescribeCampaign",
        "connect-campaigns:ListCampaigns",
        "connect:DescribeAgentStatus",
        "connect:DescribeDataTable",
```

```
        "connect:DescribeEmailAddress",
        "connect:DescribeEvaluationForm",
        "connect:DescribeHoursOfOperation",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribeMetric",
        "connect:DescribeNotification",
        "connect:DescribePhoneNumber",
        "connect:DescribePredefinedAttribute",
        "connect:DescribePrompt",
        "connect:DescribeQueue",
        "connect:DescribeQuickConnect",
        "connect:DescribeRoutingProfile",
        "connect:DescribeRule",
        "connect:DescribeSecurityProfile",
        "connect:DescribeTrafficDistributionGroup",
        "connect:DescribeUser",
        "connect:DescribeUserHierarchyGroup",
        "connect:DescribeUserHierarchyStructure",
        "connect:DescribeView",
        "connect:DescribeWorkspace",
        "connect:GetTaskTemplate",
        "connect:ListAgentStatuses",
        "connect:ListApprovedOrigins",
        "connect:ListDataTables",
        "connect:ListEvaluationForms",
        "connect:ListEvaluationFormVersions",
        "connect:ListHoursOfOperationOverrides",
        "connect:ListHoursOfOperations",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListMetrics",
        "connect:ListNotifications",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "connect:ListPredefinedAttributes",
        "connect:ListPrompts",
        "connect:ListQueueEmailAddresses",
        "connect:ListQueueQuickConnects",
        "connect:ListQueues",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileManualAssignmentQueues",
```

```
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListSecurityProfileAIAgents",
        "connect:ListSecurityProfileApplications",
        "connect:ListSecurityProfileFlowModules",
        "connect:ListSecurityProfilePermissions",
        "connect:ListSecurityProfiles",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListTrafficDistributionGroups",
        "connect:ListUserHierarchyGroups",
        "connect:ListUsers",
        "connect:ListViews",
        "connect:ListViewVersions",
        "connect:ListWorkspaceMedia",
        "connect:ListWorkspacePages",
        "connect:ListWorkspaces",
        "connect:SearchAvailablePhoneNumbers",
        "connect:SearchWorkspaceAssociations",
        "controltower:GetLandingZone",
        "controltower:ListLandingZones",
        "cur:DescribeReportDefinitions",
        "cur:ListTagsForResource",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "databrew:ListTagsForResource",
        "datasync:DescribeAgent",
        "datasync:DescribeLocationAzureBlob",
        "datasync:DescribeLocationEfs",
        "datasync:DescribeLocationFsxLustre",
        "datasync:DescribeLocationFsxOntap",
```

```
        "datasync:DescribeLocationFsxOpenZfs",
        "datasync:DescribeLocationFsxWindows",
        "datasync:DescribeLocationHdfs",
        "datasync:DescribeLocationNfs",
        "datasync:DescribeLocationObjectStorage",
        "datasync:DescribeLocationS3",
        "datasync:DescribeLocationSmb",
        "datasync:DescribeTask",
        "datasync:ListAgents",
        "datasync:ListLocations",
        "datasync:ListTagsForResource",
        "datasync:ListTasks",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentProfile",
        "datazone:GetGroupProfile",
        "datazone:GetSubscriptionTarget",
        "datazone:GetUserProfile",
        "datazone:ListDomains",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListSubscriptionTargets",
        "datazone:SearchGroupProfiles",
        "datazone:SearchUserProfiles",
        "dax:DescribeClusters",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "deadline:GetBudget",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetJob",
        "deadline:GetLicenseEndpoint",
        "deadline:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
```

```
        "deadline:GetQueueFleetAssociation",
        "deadline:GetQueueLimitAssociation",
        "deadline:GetStorageProfile",
        "deadline:ListBudgets",
        "deadline:ListFarms",
        "deadline:ListFleets",
        "deadline:ListJobs",
        "deadline:ListLicenseEndpoints",
        "deadline:ListMonitors",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListQueueLimitAssociations",
        "deadline:ListQueues",
        "deadline:ListStorageProfiles",
        "deadline:ListTagsForResource",
        "deadline:SearchJobs",
        "detective:ListGraphs",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListNetworkProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTagsForResource",
        "devicefarm:ListTestGridProjects",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListNotificationChannels",
        "directconnect:DescribeConnections",
        "dms:DescribeCertificates",
        "dms:DescribeDataMigrations",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationConfigs",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTasks",
        "dms:ListDataProviders",
        "dms:ListInstanceProfiles",
        "dms:ListMigrationProjects",
        "dms:ListTagsForResource",
```

```
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:ListTagsForResource",
        "ds:DescribeDirectories",
        "ds:DescribeDomainControllers",
        "ds:DescribeEventTopics",
        "ds:ListLogSubscriptions",
        "ds:ListTagsForResource",
        "dsql:GetCluster",
        "dsql:GetClusterPolicy",
        "dsql:GetVpcEndpointServiceName",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeTransitGatewayMeteringPolicies",
        "ec2:GetAllowedImagesSettings",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetRouteServerAssociations",
        "ec2:GetRouteServerPropagations",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayMulticastGroups",
```

```
        "ec2:SearchTransitGatewayRoutes",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribePullThroughCacheRules",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:DescribeRepositoryCreationTemplates",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:GetRepositoryPolicy",
        "ecr:ListTagsForResource",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeExpressGatewayService",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListServices",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeCapability",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:ListAddons",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListCapabilities",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "eks:ListTagsForResource",
```

```
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:DescribeCapacityReservation",
        "elasticloadbalancing:DescribeListenerAttributes",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
```

```
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "elemental-inference:GetFeed",
        "elemental-inference:ListFeeds",
        "elemental-inference:ListTagsForResource",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "entityresolution:GetIdMappingWorkflow",
        "entityresolution:GetIdNamespace",
        "entityresolution:GetMatchingWorkflow",
        "entityresolution:GetSchemaMapping",
        "entityresolution:ListIdMappingWorkflows",
        "entityresolution:ListIdNamespaces",
        "entityresolution:ListMatchingWorkflows",
        "entityresolution:ListSchemaMappings",
        "entityresolution:ListTagsForResource",
        "es:DescribeDomain",
        "es:DescribeDomains",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:GetCompatibleElasticsearchVersions",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListTags",
        "events:DescribeApiDestination",
        "events:DescribeArchive",
        "events:DescribeConnection",
        "events:DescribeEndpoint",
        "events:DescribeEventBus",
        "events:DescribeRule",
        "events:ListApiDestinations",
```

```
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "finspace:GetEnvironment",
        "finspace:ListEnvironments",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "firehose:ListTagsForDeliveryStream",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:ListExperimentTemplates",
        "fis:ListTagsForResource",
        "fis:ListTargetAccountConfigurations",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:ListPolicies",
        "fms:ListTagsForResource",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasets",
        "forecast:ListTagsForResource",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
```

```
        "frauddetector:GetVariables",
        "frauddetector:ListTagsForResource",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeFileSystems",
        "fsx:DescribeS3AccessPointAttachments",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "gamelift:DescribeAlias",
        "gamelift:DescribeBuild",
        "gamelift:DescribeContainerFleet",
        "gamelift:DescribeContainerGroupDefinition",
        "gamelift:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScalingPolicies",
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListContainerFleets",
        "gamelift:ListContainerGroupDefinitions",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListLocations",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "gamelift:ValidateMatchmakingRuleSet",
        "gameliftstreams:GetApplication",
        "gameliftstreams:GetStreamGroup",
        "gameliftstreams:ListApplications",
        "gameliftstreams:ListStreamGroups",
        "gameliftstreams:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
```

```
        "geo:DescribeKey",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListKeys",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeAcceleratorAttributes",
        "globalaccelerator:DescribeCrossAccountAttachment",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCrossAccountAttachments",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:DescribeIntegrations",
        "glue:GetBlueprint",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
```

```
        "glue:GetRegistry",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetSession",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetWorkflow",
        "glue:ListBlueprints",
        "glue:ListCrawlers",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "glue:ListSessions",
        "glue:ListTriggers",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetComponent",
        "greengrass:GetDeployment",
        "greengrass:ListComponents",
        "greengrass:ListComponentVersions",
        "greengrass:ListDeployments",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:ListConfigs",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
        "groundstation:ListTagsForResource",
        "guardduty:DescribePublishingDestination",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:GetIPSet",
        "guardduty:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
```

```
        "guardduty:GetThreatEntitySet",
        "guardduty:GetThreatIntelSet",
        "guardduty:GetTrustedEntitySet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMalwareProtectionPlans",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatEntitySets",
        "guardduty:ListThreatIntelSets",
        "guardduty:ListTrustedEntitySets",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:GetDataTransformationProfile",
        "healthlake:ListDataTransformationProfiles",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListTagsForResource",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
```

```
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListInstanceProfilesForRole",
        "iam:ListInstanceProfileTags",
        "iam:ListMFADevices",
        "iam:ListMFADeviceTags",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:GetWorkflow",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "imagebuilder:ListLifecyclePolicies",
        "imagebuilder:ListWorkflowBuildVersions",
        "imagebuilder:ListWorkflows",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetCodeSecurityScanConfiguration",
```

```
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListCodeSecurityScanConfigurations",
        "inspector2:ListFilters",
        "inspector2:ListMembers",
        "inspector2:ListTagsForResource",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "invoicing:ListProcurementPortalPreferences",
        "invoicing:ListTagsForResource",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeBillingGroup",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCertificateProvider",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJob",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:DescribeStream",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:GetCommand",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:GetV2LoggingOptions",
        "iot:ListAuthorizers",
        "iot:ListBillingGroups",
        "iot:ListCACertificates",
        "iot:ListCertificateProviders",
        "iot:ListCertificates",
        "iot:ListCommands",
```

```
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "iot:ListPackages",
        "iot:ListPackageVersions",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListThingGroups",
        "iot:ListThingTypes",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:ValidateSecurityProfileBehaviors",
        "iotanalytics:DescribeChannel",
        "iotanalytics:DescribeDataset",
        "iotanalytics:DescribeDatastore",
        "iotanalytics:DescribePipeline",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotanalytics:ListTagsForResource",
        "iotdeviceadvisor:GetSuiteDefinition",
        "iotdeviceadvisor:ListSuiteDefinitions",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotfleethub:DescribeApplication",
        "iotfleethub:ListApplications",
        "iotfleetwise:GetCampaign",
        "iotfleetwise:GetDecoderManifest",
```

```
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetStateTemplate",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:ListCampaigns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSConfigServiceRolePolicyStatementID2",
      "Effect" : "Allow",
      "Action" : [
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListStateTemplates",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeComputationModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeDataset",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModelCompositeModels",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:ListComputationModels",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListDatasets",
        "iotsitewise:ListGateways",
```

```
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:GetEntity",
        "iottwinmaker:GetScene",
        "iottwinmaker:GetSyncJob",
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListTagsForResource",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessDeviceImportTask",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListDevicesForWirelessDeviceImportTask",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDeviceImportTasks",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGateways",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:GetChannel",
        "ivs:GetComposition",
        "ivs:GetEncoderConfiguration",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
```

```
        "ivs:GetStorageConfiguration",
        "ivs:GetStreamKey",
        "ivs:ListChannels",
        "ivs:ListCompositions",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:DescribeVpcConnection",
        "kafka:GetClusterPolicy",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurations",
        "kafka:ListScramSecrets",
        "kafka:ListTagsForResource",
        "kafka:ListVpcConnections",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListTagsForResource",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra-ranking:DescribeRescoreExecutionPlan",
        "kendra-ranking:ListRescoreExecutionPlans",
        "kendra-ranking:ListTagsForResource",
        "kendra:DescribeIndex",
        "kendra:ListDataSources",
        "kendra:ListIndices",
```

```
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:GetResourcePolicy",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lakeformation:DescribeLakeFormationIdentityCenterConfiguration",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionScalingConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:ListAliases",
        "lambda:ListCapacityProviders",
```

```
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListFunctions",
        "lambda:ListFunctionUrlConfigs",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "launchwizard:GetDeployment",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListTagsForResource",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
        "lex:ListBotAliases",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListDistributedGrants",
        "license-manager:ListLicenses",
        "license-manager:ListReceivedGrants",
        "license-manager:ListTagsForResource",
        "lightsail:GetActiveNames",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
```

```
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetOperations",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeAccountPolicies",
        "logs:DescribeDeliveries",
        "logs:DescribeDeliveryDestinations",
        "logs:DescribeDeliverySources",
        "logs:DescribeDestinations",
        "logs:DescribeIndexPolicies",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeResourcePolicies",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetIntegration",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:ListIntegrations",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:ListTagsForResource",
```

```
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:GetEnvironment",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsFilter",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListAllowLists",
        "macie2:ListAutomatedDiscoveryAccounts",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindingsFilters",
        "macie2:ListTagsForResource",
        "managedblockchain:GetAccessor",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:ListAccessors",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNodes",
        "mediaconnect:DescribeBridge",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeGateway",
        "mediaconnect:GetRouterInput",
        "mediaconnect:GetRouterNetworkInterface",
        "mediaconnect:ListBridges",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGateways",
        "mediaconnect:ListRouterInputs",
        "mediaconnect:ListRouterNetworkInterfaces",
        "mediaconnect:ListRouterOutputs",
        "mediaconnect:ListTagsForResource",
        "medialive:DescribeChannelPlacementGroup",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeNode",
        "medialive:DescribeSdiSource",
        "medialive:GetCloudWatchAlarmTemplate",
```

```
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:ListChannelPlacementGroups",
        "medialive:ListCloudWatchAlarmTemplateGroups",
        "medialive:ListCloudWatchAlarmTemplates",
        "medialive:ListEventBridgeRuleTemplateGroups",
        "medialive:ListEventBridgeRuleTemplates",
        "medialive:ListMultiplexes",
        "medialive:ListMultiplexPrograms",
        "medialive:ListNodes",
        "medialive:ListSdiSources",
        "medialive:ListSignalMaps",
        "medialive:ListTagsForResource",
        "mediapackage-vod:DescribeAsset",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListAssets",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediatailor:DescribeChannel",
        "mediatailor:DescribeLiveSource",
        "mediatailor:DescribeSourceLocation",
        "mediatailor:DescribeVodSource",
        "mediatailor:GetChannelPolicy",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListChannels",
        "mediatailor:ListLiveSources",
        "mediatailor:ListPlaybackConfigurations",
        "mediatailor:ListSourceLocations",
        "mediatailor:ListVodSources",
        "medical-imaging:GetDatastore",
        "medical-imaging:ListDatastores",
        "medical-imaging:ListTagsForResource",
```

```
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListTags",
        "mobiletargeting:GetApp",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetCampaign",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetEmailChannel",
        "mobiletargeting:GetEmailTemplate",
        "mobiletargeting:GetEventStream",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:GetSegment",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTagsForResource",
        "mobiletargeting:ListTemplates",
        "mpa:GetIdentitySource",
        "mpa:ListIdentitySources",
        "mpa:ListTagsForResource",
        "mq:DescribeBroker",
        "mq:DescribeConfiguration",
        "mq:ListBrokers",
        "mq:ListConfigurations",
        "mq:ListTags",
        "neptune-graph:GetGraphSnapshot",
        "neptune-graph:ListGraphSnapshots",
        "neptune-graph:ListTagsForResource",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetDirectConnectGatewayAttachment",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
```

```
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:ListAttachments",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListCoreNetworks",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStudioComponents",
        "nimble:ListStudios",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:ListTagsForResource",
        "notifications:GetEventRule",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications:ListOrganizationalUnits",
        "notifications:ListTagsForResource",
        "nova-act:GetWorkflowDefinition",
        "nova-act:ListWorkflowDefinitions",
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListLinks",
        "oam:ListSinks",
        "oam:ListTagsForResource",
        "omics:GetAnnotationStore",
        "omics:GetConfiguration",
        "omics:GetReferenceStore",
        "omics:GetRun",
        "omics:GetRunCache",
        "omics:GetRunGroup",
        "omics:GetS3AccessPolicy",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
```

```
        "omics:GetWorkflow",
        "omics:GetWorkflowVersion",
        "omics:ListAnnotationStores",
        "omics:ListConfigurations",
        "omics:ListReferenceStores",
        "omics:ListRunCaches",
        "omics:ListRunGroups",
        "omics:ListRuns",
        "omics:ListSequenceStores",
        "omics:ListTagsForResource",
        "omics:ListVariantStores",
        "omics:ListWorkflows",
        "omics:ListWorkflowVersions",
        "opsworks:DescribeInstances",
        "opsworks:DescribeLayers",
        "opsworks:DescribeTimeBasedAutoScaling",
        "opsworks:DescribeVolumes",
        "opsworks:ListTags",
        "organizations:DescribeAccount",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "osis:GetPipeline",
        "osis:GetResourcePolicy",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "outposts:GetSite",
        "outposts:ListSites",
        "panorama:DescribeApplicationInstance",
        "panorama:DescribeApplicationInstanceDetails",
```

```
        "panorama:DescribePackage",
        "panorama:DescribePackageVersion",
        "panorama:ListApplicationInstances",
        "panorama:ListNodes",
        "panorama:ListPackages",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListServicePrincipalNames",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-ad:ListTemplateGroupAccessControlEntries",
        "pca-connector-ad:ListTemplates",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:ListChallengeMetadata",
        "pca-connector-scep:ListConnectors",
        "pca-connector-scep:ListTagsForResource",
        "pcs:GetCluster",
        "pcs:GetComputeNodeGroup",
        "pcs:GetQueue",
        "pcs:ListClusters",
        "pcs:ListComputeNodeGroups",
        "pcs:ListQueues",
        "pcs:ListTagsForResource",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "pipes:DescribePipe",
```

```
        "pipes:ListPipes",
        "profile:GetDomain",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "qbusiness:GetApplication",
        "qbusiness:GetDataSource",
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetPolicy",
        "qbusiness:GetRetriever",
        "qbusiness:GetWebExperience",
        "qbusiness:ListApplications",
        "qbusiness:ListDataSources",
        "qbusiness:ListIndices",
        "qbusiness:ListPlugins",
        "qbusiness:ListRetrievers",
        "qbusiness:ListTagsForResource",
        "qbusiness:ListWebExperiences",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeCustomPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeFolder",
        "quicksight:DescribeFolderPermissions",
        "quicksight:DescribeOAuthClientApplication",
        "quicksight:DescribeRefreshSchedule",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:DescribeTopic",
        "quicksight:DescribeVPCConnection",
        "quicksight:ListAnalyses",
```

```
        "quicksight:ListCustomPermissions",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListFolders",
        "quicksight:ListOAuthClientApplications",
        "quicksight:ListRefreshSchedules",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "quicksight:ListTopics",
        "quicksight:ListVPCConnections",
        "ram:GetPermission",
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares",
        "ram:ListPermissionAssociations",
        "ram:ListPermissions",
        "ram:ListPermissionVersions",
        "ram:ListResources",
        "ram:ListResourceSharePermissions",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBProxyTargetGroups",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeIntegrations",
        "rds:DescribeOptionGroups",
```

```
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterDbRevisions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeDataShares",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeIntegrations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeSnapshotCopyGrants",
        "redshift:DescribeTags",
        "redshift:GetResourcePolicy",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetRoute",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:DescribeCollection",
        "rekognition:DescribeProjects",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListCollections",
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionResourceMappings",
```

```
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "robomaker:DescribeRobotApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:ListRobotApplications",
        "robomaker:ListSimulationApplications",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:GetChange",
        "route53:GetDNSSEC",
```

```
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListCidrBlocks",
        "route53:ListCidrCollections",
        "route53:ListCidrLocations",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListQueryLoggingConfigs",
        "route53:ListResourceRecordSets",
        "route53:ListTagsForResource",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetOutpostResolver",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallDomains",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListOutpostResolvers",
        "route53resolver:ListResolverDnssecConfigs",
        "route53resolver:ListResolverEndpointIpAddresses",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRuleAssociations",
        "route53resolver:ListResolverRules",
        "route53resolver:ListTagsForResource",
        "rtbfabric:GetCertificateAssociation",
        "rtbfabric:GetInboundExternalLink",
```

```
        "rtbfabric:GetLink",
        "rtbfabric:GetLinkRoutingRule",
        "rtbfabric:GetOutboundExternalLink",
        "rtbfabric:GetRequesterGateway",
        "rtbfabric:GetResponderGateway",
        "rtbfabric:ListCertificateAssociations",
        "rtbfabric:ListLinkRoutingRules",
        "rtbfabric:ListLinks",
        "rtbfabric:ListRequesterGateways",
        "rtbfabric:ListResponderGateways",
        "rtbfabric:ListTagsForResource",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:ListTagsForResource",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListRegionalBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
```

```
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsInstances",
        "s3:ListAccessGrantsLocations",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3:ListTagsForResource",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
        "s3express:GetAccessPointScope",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:GetMetricsConfiguration",
        "s3express:ListAccessPointsForDirectoryBuckets",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:ListTagsForResource",
        "s3files:GetAccessPoint",
        "s3files:GetFileSystem",
        "s3files:GetFileSystemPolicy",
        "s3files:GetMountTarget",
        "s3files:GetSynchronizationConfiguration",
        "s3files:ListAccessPoints",
        "s3files:ListFileSystems",
```

```
        "s3files:ListMountTargets",
        "s3files:ListTagsForResource",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketMetricsConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableBucketReplication",
        "s3tables:GetTableBucketStorageClass",
        "s3tables:ListTableBuckets",
        "s3tables:ListTagsForResource",
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:ListIndexes",
        "s3vectors:ListTagsForResource",
        "s3vectors:ListVectorBuckets",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeClusterSchedulerConfig",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeComputeQuota",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHub",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeInferenceExperiment",
```

```
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeMlflowApp",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelCardExportJob",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribeOptimizationJob",
        "sagemaker:DescribePartnerApp",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeStudioLifecycleConfig",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTrainingPlan",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListClusters",
        "sagemaker:ListClusterSchedulerConfigs",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListComputeQuotas",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDomains",
```

```
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHubs",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImages",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListMlflowApps",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCardExportJobs",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelCardVersions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListOptimizationJobs",
        "sagemaker:ListPartnerApps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSpaces",
        "sagemaker:ListStudioLifecycleConfigs",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingPlans",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
```

```
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "sdb:GetAttributes",
        "sdb:ListDomains",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetTargetDomains",
        "securityagent:GetApplication",
        "securityagent:ListApplications",
        "securityagent:ListPentests",
        "securityagent:ListTagsForResource",
        "securityagent:ListTargetDomains",
        "securityhub:DescribeHub",
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeStandardsControls",
        "securityhub:GetAggregatorV2",
        "securityhub:GetAutomationRuleV2",
        "securityhub:GetConfigurationPolicy",
        "securityhub:GetConfigurationPolicyAssociation",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindingAggregator",
        "securityhub:ListAggregatorsV2",
        "securityhub:ListAutomationRulesV2",
        "securityhub:ListConfigurationPolicies",
        "securityhub:ListConfigurationPolicyAssociations",
        "securityhub:ListEnabledProductsForImport",
        "securityhub:ListFindingAggregators",
        "securityhub:ListTagsForResource",
        "securitylake:GetSubscriber",
        "securitylake:ListDataLakeExceptions",
        "securitylake:ListDataLakes",
```

```
        "securitylake:ListLogSources",
        "securitylake:ListSubscribers",
        "securitylake:ListTagsForResource",
        "serviceCatalog:DescribePortfolioShares",
        "servicecatalog:DescribeServiceAction",
        "servicecatalog:DescribeTagOption",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListApplications",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:ListServiceActions",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:ListTagOptions",
        "servicediscovery:GetInstance",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:ListInstances",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
        "ses:DescribeReceiptRuleSet",
        "ses:GetAddonInstance",
        "ses:GetAddonSubscription",
        "ses:GetAddressList",
        "ses:GetArchive",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailTemplate",
        "ses:GetIngressPoint",
        "ses:GetRelay",
        "ses:GetRuleSet",
        "ses:GetTemplate",
        "ses:GetTrafficPolicy",
        "ses:ListAddonInstances",
        "ses:ListAddonSubscriptions",
        "ses:ListAddressLists",
        "ses:ListArchives",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
```

```
        "ses:ListDedicatedIpPools",
        "ses:ListEmailTemplates",
        "ses:ListIngressPoints",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListRelays",
        "ses:ListRuleSets",
        "ses:ListTagsForResource",
        "ses:ListTemplates",
        "ses:ListTrafficPolicies",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeProtectionGroup",
        "shield:DescribeSubscription",
        "shield:ListProtectionGroups",
        "shield:ListTagsForResource",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningProfiles",
        "sms-voice:DescribeConfigurationSets",
        "sms-voice:DescribeKeywords",
        "sms-voice:DescribeOptOutLists",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeProtectConfigurations",
        "sms-voice:DescribeSenderIds",
        "sms-voice:GetProtectConfigurationCountryRuleSet",
        "sms-voice:GetResourcePolicy",
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "sns:GetDataProtectionPolicy",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:GetRotation",
```

```
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListRotations",
        "ssm-contacts:ListTagsForResource",
        "ssm-guiconnect:GetConnectionRecordingPreferences",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-sap:ListTagsForResource",
        "ssm:DescribeAssociation",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeParameters",
        "ssm:DescribePatchBaselines",
        "ssm:GetAutomationExecution",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetMaintenanceWindow",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:GetServiceSetting",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "sso:DescribeApplication",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetPermissionsBoundaryForPermissionSet",
        "sso:ListApplications",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
```

```
        "states:DescribeStateMachineAlias",
        "states:ListActivities",
        "states:ListStateMachineAliases",
        "states:ListStateMachines",
        "states:ListStateMachineVersions",
        "states:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:ListTagsForResource",
        "storagegateway:ListVolumes",
        "sts:GetCallerIdentity",
        "support:DescribeCases",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "textract:GetAdapter",
        "textract:ListAdapters",
        "textract:ListTagsForResource",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:ListTagsForResource",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transcribe:GetCallAnalyticsJob",
        "transcribe:GetVocabularyFilter",
        "transcribe:ListCallAnalyticsJobs",
        "transcribe:ListTagsForResource",
        "transcribe:ListVocabularyFilters",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
```

```
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWebApp",
        "transfer:DescribeWebAppCustomization",
        "transfer:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListTagsForResource",
        "transfer:ListUsers",
        "transfer:ListWebApps",
        "transfer:ListWorkflows",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "verifiedpermissions:ListTagsForResource",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourceConfiguration",
        "vpc-lattice:GetResourceGateway",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkResourceAssociation",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListResourceConfigurations",
        "vpc-lattice:ListResourceGateways",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworkResourceAssociations",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
```

```
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:GetWebACL",
        "waf-regional:GetWebACLForResource",
        "waf-regional:ListLoggingConfigurations",
        "waf:GetLoggingConfiguration",
        "waf:GetWebACL",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRuleGroup",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "wisdom:GetAIAgent",
        "wisdom:GetAIGuardrail",
        "wisdom:GetAIPrompt",
        "wisdom:GetAssistant",
        "wisdom:ListAIAgentVersions",
        "wisdom:ListAIGuardrails",
        "wisdom:ListAIGuardrailVersions",
        "wisdom:ListAIPromptVersions",
        "wisdom:ListAssistants",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIpAccessSettings",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListUserSettings",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetIndexingRules",
        "xray:GetSamplingRules",
```

```
        "xray:GetTraceSegmentDestination",
        "xray:ListResourcePolicies",
        "xray:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSConfigSLRLogStatementID",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*"
    },
    {
      "Sid" : "AWSConfigSLRLogEventStatementID",
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
    },
    {
      "Sid" : "AWSConfigSLRApiGatewayStatementID",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/resources",
```

```
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/v2/apis/*/routes",
        "arn:aws:apigateway:*::/v2/apis/*/routes/*",
        "arn:aws:apigateway:*::/v2/apis",
        "arn:aws:apigateway:*::/v2/apis/*",
        "arn:aws:apigateway:*::/v2/apis/*/integrations",
        "arn:aws:apigateway:*::/v2/apis/*/integrations/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSConfigThirdPartyServiceRolePolicy

Deskripsi: Memberikan izin untuk AWS Config untuk inventarisasi dan mengevaluasi kepatuhan sumber daya cloud pihak ketiga.

`AWSConfigThirdPartyServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 22 Juni 2026, 17:57 UTC
- Waktu teredit: 22 Juni 2026, 17:57 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigThirdPartyServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowGetWebIdentityTokenByConfig",
      "Effect" : "Allow",
      "Action" : "sts:GetWebIdentityToken",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "sts:IdentityTokenAudience" : [
            "api://AzureADTokenExchange"
          ]
        }
      }
    },
    {
      "Sid" : "AllowConfigActionsForRules",
      "Effect" : "Allow",
      "Action" : [
        "config:PutEvaluations",
        "config:GetComplianceDetailsByConfigRule"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCloudwatchActionsForMetrics",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Config"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSConfigUserAccess

Deskripsi: Menyediakan akses untuk menggunakan AWS Config, termasuk mencari berdasarkan tag pada sumber daya, dan membaca semua tag. Ini tidak memberikan izin untuk mengkonfigurasi AWS Config, yang memerlukan hak administratif.

`AWSConfigUserAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSConfigUserAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Februari 2015, 19:38 UTC
- Waktu teredit: 18 Maret 2019, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConfigUserAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "config:Select*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

Konektor AWS

Deskripsi: Mengaktifkan read/write akses luas ke SEMUA objek EC2, read/write akses ke bucket S3 dimulai dengan 'import-to-ec2-', dan kemampuan untuk membuat daftar semua bucket S3, agar AWS Konektor dapat mengimpor VM atas nama Anda.

`AWSConnector`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSConnector` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Februari 2015, 17:14 UTC
- Waktu teredit: 28 September 2015, 19.50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConnector`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:AbortMultipartUpload",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : "arn:aws:s3:::import-to-ec2-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelConversionTask",
        "ec2:CancelExportTask",
        "ec2:CreateImage",
        "ec2:CreateInstanceExportTask",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteTags",
        "ec2:DeleteVolume",
        "ec2:DescribeConversionTasks",
        "ec2:DescribeExportTasks",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "ec2:DetachVolume",
        "ec2:ImportInstance",
        "ec2:ImportVolume",
        "ec2:ModifyInstanceAttribute",
```

```
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ImportImage",
        "ec2:DescribeImportImageTasks",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:CancelImportTask",
        "ec2:ImportSnapshot",
        "ec2:DescribeImportSnapshotTasks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSControlTowerAccountServiceRolePolicy

Deskripsi: Men AWS gizinkan Control Tower untuk memang AWS gil layanan yang menyediakan konfigurasi akun otomatis dan tata kelola terpusat atas nama Anda.

`AWSControlTowerAccountServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 05 Juni 2023, 22:04 UTC
- Waktu yang diedit: 20 Mei 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutRuleOnSpecificSourcesAndDetailTypes",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "events:source" : "aws.securityhub"
        },
        "ForAllValues:StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported"
        },
        "Null" : {
          "events:detail-type" : "false"
```

```
        },
        "StringEquals" : {
          "events:ManagedBy" : "controltower.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowOtherOperationsOnRulesManagedByControlTower",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "controltower.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowDescribeOperationsOnRulesManagedByControlTower",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*"
    },
    {
      "Sid" : "AllowControlTowerToPublishSecurityNotifications",
      "Effect" : "Allow",
      "Action" : "sns:publish",
      "Resource" : "arn:aws:sns:*:*:aws-controltower-AggregateSecurityNotifications",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "AllowActionsForSecurityHubIntegration",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:DescribeStandardsControls",
        "securityhub:GetEnabledStandards"
      ],
      "Resource" : "arn:aws:securityhub:*:*:hub/default"
    },
    {
      "Sid" : "AllowDeleteConfigRule",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*"
    },
    {
      "Sid" : "AllowPutConfigRule",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*"
    },
    {
      "Sid" : "AllowConfigTagResource",
      "Effect" : "Allow",
      "Action" : [
        "config:TagResource"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws-control-tower" : "managed-by-control-tower"
        }
      }
    },
    {
      "Sid" : "AllowConfigRulesDescribe",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigRules"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AllowControlTowerToCreateConfigAggregator",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigurationAggregator"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
controltower.amazonaws.com/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowControlTowerToManageConfigAggregator",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigurationAggregator",
        "config:DescribeAggregateComplianceByConfigRules",
        "config:SelectAggregateResourceConfig"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
controltower.amazonaws.com/config-aggregator-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowControlTowerToTagConfigAggregator",
      "Effect" : "Allow",
      "Action" : [
        "config:TagResource"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
controltower.amazonaws.com/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws-control-tower" : "managed-by-control-tower",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowControlTowerToPassAggregatorRoleToConfig",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "config.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDescribeConfigurationAggregators",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationAggregators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowListDelegatedAdministratorsForConfig",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "config.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowListDescribeOrganization",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowActionsForCloudFormationHooksIntegration",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:SetTypeConfiguration",
        "cloudformation:DeactivateType",
        "cloudformation:ActivateType"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:type/hook/AWS-ControlTower*"
    },
    {
      "Sid" : "AllowBatchDescribeTypeConfigurationsForHookConfigFetch",
      "Effect" : "Allow",
      "Action" : "cloudformation:BatchDescribeTypeConfigurations",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSControlTowerCloudTrailRolePolicy

Deskripsi: Menara AWS Kontrol memungkinkan AWS CloudTrail sebagai praktik terbaik dan memberikan peran ini kepada AWS CloudTrail. AWS CloudTrail mengambil peran ini untuk membuat dan menerbitkan CloudTrail log

`AWSControlTowerCloudTrailRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSControlTowerCloudTrailRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 November 2025, 21:19 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerCloudTrailRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogStream",
      "Resource" : "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs*:*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSControlTowerIdentityCenterManagementPolicy

Deskripsi: Memberikan izin untuk mengelola sumber daya Pusat Identitas IAM (iDC) di akun anggota yang terdaftar dengan AWS Control Tower. Kebijakan ini dilampirkan pada AWSControlTowerAdmin peran hanya jika pelanggan telah memilih integrasi IAM iDC di Zona Pendaratan Menara Kontrol mereka AWS .

`AWSControlTowerIdentityCenterManagementPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSControlTowerIdentityCenterManagementPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 03 Oktober 2025, 18:34 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerIdentityCenterManagementPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowIdentityCenterInstancePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListPermissionSets"
      ],
      "Resource" : "arn:aws:sso:::instance/*"
    },
    {
      "Sid" : "AllowIdentityCenterManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:ListDirectoryAssociations",
        "sso:ListProfileAssociations",
        "sso:AssociateProfile",
        "sso:GetProfile",
        "sso:CreateProfile",
        "sso:UpdateProfile",
        "sso:GetTrust",
        "sso:CreateTrust",
        "sso:UpdateTrust",
        "sso:CreateApplicationInstance",
        "sso:GetApplicationInstance",
        "sso:GetSSOStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowIdentityCenterDirectoryPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:SearchGroups",
        "sso-directory:CreateGroup",
        "sso-directory:SearchUsers",
        "sso-directory:CreateUser",
        "sso-directory:DescribeDirectory"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSControlTowerServiceRolePolicy

Deskripsi: Menyediakan akses ke AWS Sumber Daya yang dikelola atau digunakan oleh AWS Control Tower

`AWSControlTowerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSControlTowerServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 03 Mei 2019, 18:19 UTC
- Waktu teredit: 10 September 2026, 19:47 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v22 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CreateStackInstances",
        "cloudformation:CreateStackSet",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateStackInstances",
        "cloudformation:UpdateStackSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:type/resource/AWS-IAM-Role"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
```

```
        "cloudformation:CreateStackInstances",
        "cloudformation:CreateStackSet",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackInstances",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateStackInstances",
        "cloudformation:UpdateStackSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/AWSControlTower*/*",
        "arn:aws:cloudformation:*:*:stack/StackSet-AWSControlTower*/*",
        "arn:aws:cloudformation:*:*:stackset/AWSControlTower*:*",
        "arn:aws:cloudformation:*:*:stackset-target/AWSControlTower*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateTrail",
        "cloudtrail:DeleteTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudtrail:UpdateTrail",
        "cloudtrail:PutEventSelectors",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs*:*",
        "arn:aws:cloudtrail:*:*:trail/aws-controltower*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-controltower*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSControlTowerExecution",
        "arn:aws:iam::*:role/AWSControlTowerBlueprintAccess"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "ec2:DescribeAvailabilityZones",
        "iam:ListRoles",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "organizations:CreateAccount",
        "organizations:DescribeAccount",
        "organizations:DescribeCreateAccountStatus",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListRoots",
        "organizations:MoveAccount",
        "servicecatalog:AssociatePrincipalWithPortfolio"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetUser",
        "iam:ListAttachedRolePolicies",
        "iam:GetRolePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSControlTowerStackSetRole",
        "arn:aws:iam::*:role/service-role/AWSControlTowerCloudTrailRole",
        "arn:aws:iam::*:role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigurationAggregator",
        "config:PutConfigurationAggregator",
        "config:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/aws-control-tower" : "managed-by-control-tower"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "config.amazonaws.com",
            "cloudtrail.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "account:EnableRegion",
        "account:ListRegions",
        "account:GetRegionOptStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCloudFormationHooksIntegration",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:SetTypeConfiguration",
        "cloudformation:DeactivateType",
        "cloudformation:ActivateType"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:type/hook/AWS-ControlTower*"
    },
    {
      "Sid" : "AllowBatchDescribeTypeConfigurationsForHookConfigFetch",
      "Effect" : "Allow",
      "Action" : "cloudformation:BatchDescribeTypeConfigurations",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowActionsForCloudFormationStackSetOrganizationsTrustedAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ActivateOrganizationsAccess",
        "cloudformation:DescribeOrganizationsAccess"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:type/resource/AWS-IAM-Role",
        "arn:aws:cloudformation:*:*:stack/AWSControlTower*/*",
        "arn:aws:cloudformation:*:*:stack/StackSet-AWSControlTower*/*",
        "arn:aws:cloudformation:*:*:stackset/AWSControlTower*:*",
        "arn:aws:cloudformation:*:*:stackset-target/AWSControlTower*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack",
            "UpdateStack"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSCostAndUsageReportAutomationPolicy

Deskripsi: Memberikan izin untuk mendeskripsikan organisasi akun, membuat bucket S3 untuk program MAP dan menerapkan tag padanya, membuat Laporan Biaya dan Penggunaan, dan menjelaskan definisi Laporan Biaya dan Penggunaan.

`AWSCostAndUsageReportAutomationPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCostAndUsageReportAutomationPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 November 2021, 21:27 UTC
- Waktu teredit: 01 November 2021, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketTagging",
        "s3:PutBucketTagging",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:CreateBucket"
      ],
      "Resource" : "arn:aws:s3:::aws-map-cur-bucket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cur:PutReportDefinition",
        "cur:DeleteReportDefinition",
        "cur:DescribeReportDefinitions"
      ],
      "Resource" : "arn:aws:cur:*:*:definition/map-migrated-report"
    },
    {
      "Effect" : "Allow",
      "Action" : "cur:DescribeReportDefinitions",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDataExchangeDataGrantOwnerFullAccess

Deskripsi: Memberi pemilik Data Grant akses ke tindakan Pertukaran AWS Data menggunakan Konsol Manajemen AWS dan SDK.

`AWSDataExchangeDataGrantOwnerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataExchangeDataGrantOwnerFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Oktober 2024, 14:43 UTC
- Waktu teredit: 24 Oktober 2024, 14:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeDataGrantOwnerFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateDataSet",
        "dataexchange:UpdateDataSet",
        "dataexchange:GetDataSet",
        "dataexchange:DeleteDataSet",
```

```
        "dataexchange:ListDataSets",
        "dataexchange:CreateRevision",
        "dataexchange:UpdateRevision",
        "dataexchange:GetRevision",
        "dataexchange:DeleteRevision",
        "dataexchange:RevokeRevision",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:CreateAsset",
        "dataexchange:UpdateAsset",
        "dataexchange:GetAsset",
        "dataexchange:DeleteAsset",
        "dataexchange:ListRevisionAssets",
        "dataexchange:SendApiAsset",
        "dataexchange:CreateDataGrant",
        "dataexchange:GetDataGrant",
        "dataexchange:DeleteDataGrant",
        "dataexchange:ListDataGrants",
        "dataexchange:PublishToDataGrant",
        "dataexchange:SendDataSetNotification",
        "dataexchange:TagResource",
        "dataexchange:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeJobsActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "IMPORT_ASSETS_FROM_S3",
            "IMPORT_ASSET_FROM_SIGNED_URL",
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "IMPORT_ASSET_FROM_API_GATEWAY_API",
            "IMPORT_ASSETS_FROM_REDSHIFT_DATA_SHARES",
            "IMPORT_ASSETS_FROM_LAKE_FORMATION_TAG_POLICY"
          ]
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDataExchangeDataGrantReceiverFullAccess

Deskripsi: Memberikan akses penerima AWS Data Grant ke tindakan Pertukaran Data menggunakan Konsol Manajemen AWS dan SDK.

`AWSDataExchangeDataGrantReceiverFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataExchangeDataGrantReceiverFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Oktober 2024, 14:45 UTC
- Waktu teredit: 24 Oktober 2024, 14:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeDataGrantReceiverFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:GetDataSet",
        "dataexchange:ListDataSets",
        "dataexchange:GetRevision",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:GetAsset",
        "dataexchange:ListRevisionAssets",
        "dataexchange:SendApiAsset"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeExportActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "EXPORT_REVISIONS_TO_S3"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "DataExchangeEventActionActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateEventAction",
        "dataexchange:UpdateEventAction",
        "dataexchange:DeleteEventAction",
        "dataexchange:GetEventAction",
        "dataexchange:ListEventActions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeDataGrantActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:AcceptDataGrant",
        "dataexchange:ListReceivedDataGrants",
        "dataexchange:GetReceivedDataGrant"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDataExchangeFullAccess

Deskripsi: Memberikan akses penuh ke Pertukaran AWS Data dan AWS Marketplace tindakan menggunakan Konsol Manajemen AWS dan SDK. Ini juga menyediakan akses pilihan ke layanan terkait yang diperlukan untuk mengambil keuntungan penuh dari Per AWS tukaran Data.

`AWSDataExchangeFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataExchangeFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 November 2019, 19:27 UTC
- Waktu teredit: 24 Juni 2024, 19:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeFullAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3GetActionConditionalResourceAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3GetActionConditionalTagAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/AWSDataExchange" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3WriteActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3ReadActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceProviderActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:UpdateAgreementApprovalRequest",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms",
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceSubscriberActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListPrivateListings",
        "aws-marketplace:DescribeAgreement"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftConditionalActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "redshift:ConsumerIdentifier" : "ADX"
        }
      }
    },
    {
      "Sid" : "RedshiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeDataSharesForProducer",
        "redshift:DescribeDataShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayActions",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDataExchangeProviderFullAccess

Deskripsi: Memberikan akses penyedia AWS data ke Data Exchange dan AWS Marketplace tindakan menggunakan Konsol Manajemen AWS dan SDK. Ini juga menyediakan akses pilihan ke layanan terkait yang diperlukan untuk mengambil keuntungan penuh dari Per AWS tukaran Data.

`AWSDataExchangeProviderFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataExchangeProviderFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 November 2019, 19:27 UTC
- Waktu teredit: 15 Agustus 2024, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "DataExchangeActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateDataSet",
        "dataexchange:CreateRevision",
        "dataexchange:CreateAsset",
        "dataexchange:Get*",
        "dataexchange:Update*",
        "dataexchange:List*",
        "dataexchange:Delete*",
        "dataexchange:TagResource",
        "dataexchange:UntagResource",
        "dataexchange:PublishDataSet",
        "dataexchange:SendApiAsset",
        "dataexchange:RevokeRevision",
        "dataexchange:SendDataSetNotification",
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeJobsActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "IMPORT_ASSETS_FROM_S3",
            "IMPORT_ASSET_FROM_SIGNED_URL",
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "IMPORT_ASSET_FROM_API_GATEWAY_API",
            "IMPORT_ASSETS_FROM_REDSHIFT_DATA_SHARES"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "S3GetActionConditionalResourceAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3GetActionConditionalTagAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/AWSDataExchange" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3WriteActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "S3ReadActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:UpdateAgreementApprovalRequest",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSActions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftConditionalActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "redshift:ConsumerIdentifier" : "ADX"
        }
      }
    },
    {
      "Sid" : "RedshiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeDataSharesForProducer",
        "redshift:DescribeDataShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayActions",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDataExchangeReadOnly

Deskripsi: Memberikan akses baca-saja ke AWS Data Exchange dan AWS Marketplace tindakan menggunakan Konsol Manajemen AWS dan SDK.

`AWSDataExchangeReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataExchangeReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 November 2019, 19:27 UTC
- Waktu teredit: 24 Oktober 2024, 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeReadOnly`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:GetAsset",
        "dataexchange:GetDataSet",
        "dataexchange:GetEventAction",
        "dataexchange:GetJob",
        "dataexchange:GetRevision",
        "dataexchange:GetDataGrant",
        "dataexchange:GetReceivedDataGrant",
        "dataexchange:ListDataGrants",
        "dataexchange:ListReceivedDataGrants",
```

```
        "dataexchange:ListDataSetRevisions",
        "dataexchange:ListDataSets",
        "dataexchange:ListEventActions",
        "dataexchange:ListJobs",
        "dataexchange:ListRevisionAssets",
        "dataexchange:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms",
        "aws-marketplace:ListPrivateListings",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDataExchangeServiceRolePolicyForLicenseManagement

Deskripsi: Memungkinkan AWS Pertukaran Data untuk mengakses Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh AWS Pertukaran Data untuk pengelolaan lisensi.

`AWSDataExchangeServiceRolePolicyForLicenseManagement`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 10 Oktober 2024, 14:54 UTC
- Waktu teredit: 10 Oktober 2024, 14:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataExchangeServiceRolePolicyForLicenseManagement`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowLicenseManagerActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:DescribeOrganization",
        "license-manager:ListDistributedGrants",
        "license-manager:GetGrant",
        "license-manager:CreateGrantVersion",
        "license-manager:DeleteGrant"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDataExchangeServiceRolePolicyForOrganizationDiscovery

Deskripsi: Men AWS gizinkan Pertukaran Data membaca data tentang AWS Organisasi Anda untuk menentukan kelayakan untuk distribusi lisensi pemberian AWS data Exchange Data.

`AWSDataExchangeServiceRolePolicyForOrganizationDiscovery`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 10 Oktober 2024, 14:33 UTC
- Waktu teredit: 10 Oktober 2024, 14:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataExchangeServiceRolePolicyForOrganizationDiscovery`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAWSOrganizationsActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDataExchangeSubscriberFullAccess

Deskripsi: Memberikan akses pelanggan AWS data ke Data Exchange dan AWS Marketplace tindakan menggunakan Konsol Manajemen AWS dan SDK. Ini juga menyediakan akses pilihan ke layanan terkait yang diperlukan untuk mengambil keuntungan penuh dari Per AWS tukaran Data.

`AWSDataExchangeSubscriberFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataExchangeSubscriberFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 November 2019, 19:27 UTC
- Waktu teredit: 21 Mei 2024, 17:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:Get*",
        "dataexchange:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeExportActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
```

```
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "EXPORT_REVISIONS_TO_S3"
          ]
        }
      }
    },
    {
      "Sid" : "DataExchangeEventActionActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateEventAction",
        "dataexchange:UpdateEventAction",
        "dataexchange:DeleteEventAction",
        "dataexchange:SendApiAsset"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3GetActionConditionalResourceAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3ReadActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceSubscriberActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSActions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDataLifecycleManagerServiceRole

Deskripsi: Memberikan izin yang sesuai untuk AWS Data Lifecycle Manager untuk mengambil tindakan pada AWS sumber daya

`AWSDataLifecycleManagerServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataLifecycleManagerServiceRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Juli 2018, 19:34 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRole`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots",
        "ec2:DeleteSnapshot",
```

```
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ec2:EnableFastSnapshotRestores",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DisableFastSnapshotRestores",
        "ec2:CopySnapshot",
        "ec2:ModifySnapshotAttribute",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:ModifySnapshotTier",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AwsDataLifecycleRule.managed-cwe.*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDataLifecycleManagerServiceRoleForAMIManagement

Deskripsi: Memberikan izin yang sesuai untuk Manajer Siklus Hidup AWS Data untuk mengambil tindakan pada AWS sumber daya untuk Manajemen AMI

`AWSDataLifecycleManagerServiceRoleForAMIManagement`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataLifecycleManagerServiceRoleForAMIManagement` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 21 Oktober 2020, 19:39 UTC
- Waktu teredit: 19 Agustus 2021, 17.03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRoleForAMIManagement`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ResetImageAttribute",
        "ec2:DeregisterImage",
        "ec2:CreateImage",
        "ec2:CopyImage",
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableImageDeprecation",
        "ec2:DisableImageDeprecation"
      ],
      "Resource" : "arn:aws:ec2:*::image/*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDataLifecycleManagerSSMFullAccess

Deskripsi: Memberikan izin Amazon Data Lifecycle Manager untuk melakukan tindakan Manajer Sistem yang diperlukan untuk menjalankan skrip pra dan pasca pada semua instans Amazon EC2.

`AWSDataLifecycleManagerSSMFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataLifecycleManagerSSMFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 31 Oktober 2023, 20:29 UTC
- Waktu teredit: 16 November 2023, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerSSMFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSSMReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:ListCommands",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowTaggedSSMDocumentsOnly",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DLMScriptsAccess" : "true"
        }
      }
    },
    {
      "Sid" : "AllowSpecificAWSOwnedSSMDocuments",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ssm:*:*:document/AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA"
```

```
      ]
    },
    {
      "Sid" : "AllowAllEC2Instances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDataPipeline_FullAccess

Deskripsi: Menyediakan akses penuh ke Pipeline Data, akses daftar untuk peran S3, DynamoDB, Redshift, RDS, SNS, dan IAM, dan akses PassRole untuk Peran default.

`AWSDataPipeline_FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataPipeline_FullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Januari 2017, 23:14 UTC
- Waktu teredit: 17 Agustus 2017, 18:48 UTC

- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_FullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:List*",
        "dynamodb:DescribeTable",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "sns:ListTopics",
        "sns:Subscribe",
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfiles",
        "datapipeline:*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
        "arn:aws:iam::*:role/DataPipelineDefaultRole"
```

```
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDataPipeline_PowerUser

Deskripsi: Menyediakan akses penuh ke Pipeline Data, akses daftar untuk peran S3, DynamoDB, Redshift, RDS, SNS, dan IAM, dan akses PassRole untuk Peran default.

`AWSDataPipeline_PowerUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataPipeline_PowerUser` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Januari 2017, 23:16 UTC
- Waktu teredit: 17 Agustus 2017, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_PowerUser`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:List*",
        "dynamodb:DescribeTable",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "sns:ListTopics",
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfiles",
        "datapipeline:*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
        "arn:aws:iam::*:role/DataPipelineDefaultRole"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDataSyncDiscoveryServiceRolePolicy

Deskripsi: Men DataSync gizinkan Discovery untuk berintegrasi dengan AWS layanan lain atas nama Anda.

`AWSDataSyncDiscoveryServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 20 Maret 2023, 22:19 UTC
- Waktu teredit: 20 Maret 2023, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncDiscoveryServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
```

```
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "datasync",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync:log-stream:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDataSyncFullAccess

Deskripsi: Menyediakan akses penuh AWS DataSync dan akses minimal ke dependensinya

`AWSDataSyncFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataSyncFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Januari 2019, 19:40 UTC
- Waktu teredit: 12 Februari 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncFullAccess`

Versi kebijakan

Versi kebijakan: v16 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataSyncFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "datasync:*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRegions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyNetworkInterfaceAttribute",
```

```
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "iam:GetRole",
        "iam:ListRoles",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "outposts:ListOutposts",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListRegionalBuckets",
        "secretsmanager:ListSecrets",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataSyncPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "datasync.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DataSyncCreateSLRPermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/datasync.amazonaws.com/
AWSServiceRoleForDataSync",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "datasync.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataSyncSecretsManagerCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:aws-datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataSyncSecretsManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:aws-datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "aws-
datasync",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDataSyncReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke AWS DataSync

`AWSDataSyncReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataSyncReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Januari 2019, 19:18 UTC
- Waktu teredit: 30 Juni 2020, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "datasync:Describe*",
        "datasync:List*",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "iam:GetRole",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDataSyncServiceRolePolicy

Deskripsi: Memungkinkan DataSync untuk berintegrasi dengan AWS layanan lain atas nama Anda

`AWSDataSyncServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 09 Oktober 2024, 17:45 UTC
- Waktu teredit: 15 April 2025, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataSyncCloudWatchLogCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync*"
      ]
    },
    {
      "Sid" : "DataSyncCloudWatchLogStreamUpdateAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync*:log-stream:*"
```

```
      ]
    },
    {
      "Sid" : "DataSyncSecretsManagerReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:aws-datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "aws-
datasync",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDeadlineCloud-FleetWorker

Deskripsi: Men AWS yediakan akses pekerja Deadline Cloud untuk menjalankan tugas di peternakan.

`AWSDeadlineCloud-FleetWorker`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeadlineCloud-FleetWorker` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 01 April 2024, 17:21 UTC
- Waktu teredit: 01 April 2024, 17:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-FleetWorker`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RunTasksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeFleetRoleForWorker",
        "deadline:UpdateWorker",
        "deadline:UpdateWorkerSchedule",
        "deadline:BatchGetJobEntity",
        "deadline:AssumeQueueRoleForWorker"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDeadlineCloud-UserAccessFarms

Deskripsi: Menyediakan akses workstation pengguna ke peternakan Dead AWS line Cloud dengan Read-Only izin terbatas untuk memanggil layanan lain yang diperlukan. Lampirkan kebijakan ini ke peran pengguna yang terkait dengan studio Anda.

`AWSDeadlineCloud-UserAccessFarms`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeadlineCloud-UserAccessFarms` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 April 2024, 16:54 UTC
- Waktu teredit: 29 Mei 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFarms`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "deadline:GetMonitorSettings",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFarm",
        "deadline:AssociateMemberToFleet",
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue",
        "deadline:CreateBudget",
        "deadline:DeleteBudget",
        "deadline:DisassociateMemberFromFarm",
        "deadline:DisassociateMemberFromFleet",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue",
        "deadline:GetBudget",
        "deadline:GetSessionsStatisticsAggregation",
        "deadline:ListBudgets",
        "deadline:StartSessionsStatisticsAggregation",
        "deadline:UpdateBudget"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFarm",
        "deadline:AssociateMemberToFleet",
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromFarm",
        "deadline:DisassociateMemberFromFleet",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue"
      ],
```

```
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFarmMembers",
        "deadline:ListFleetMembers",
        "deadline:ListJobMembers",
        "deadline:ListQueueMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
        "deadline:UpdateStep",
        "deadline:UpdateTask"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "OwnerManagerContributorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeQueueRoleForUser",
        "deadline:CreateJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR"
          ]
        }
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeFleetRoleForRead",
        "deadline:AssumeQueueRoleForRead",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetJob",
        "deadline:GetJobTemplate",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetStorageProfile",
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",
        "deadline:GetVolume",
        "deadline:GetWorker",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
```

```
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListSessionsForWorker",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListStorageProfiles",
        "deadline:ListStorageProfilesForQueue",
        "deadline:ListTasks",
        "deadline:ListVolumes",
        "deadline:ListWorkers",
        "deadline:SearchJobs",
        "deadline:SearchSteps",
        "deadline:SearchTasks",
        "deadline:SearchWorkers"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFarms",
        "deadline:ListFleets",
        "deadline:ListJobs",
        "deadline:ListQueues"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDeadlineCloud-UserAccessFleets

Deskripsi: Menyediakan akses workstation pengguna ke AWS armada Deadline Cloud dengan Read-Only izin terbatas untuk memanggil layanan lain yang diperlukan. Lampirkan kebijakan ini ke peran pengguna yang terkait dengan studio Anda.

`AWSDeadlineCloud-UserAccessFleets`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeadlineCloud-UserAccessFleets` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 April 2024, 17:01 UTC
- Waktu yang diedit: 29 Mei 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFleets`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFleet",
        "deadline:DisassociateMemberFromFleet"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFleet"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromFleet"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
```

```
            "VIEWER",
            ""
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFleetMembers"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
        }
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeFleetRoleForRead",
        "deadline:GetFleet",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetVolume",
        "deadline:GetWorker",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListSessionsForWorker",
        "deadline:ListVolumes",
        "deadline:ListWorkers",
        "deadline:SearchWorkers"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "deadline:FleetMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFleets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDeadlineCloud-UserAccessJobs

Deskripsi: Menyediakan akses workstation pengguna ke pekerjaan Dead AWS line Cloud dengan Read-Only izin terbatas untuk memanggil layanan lain yang diperlukan. Lampirkan kebijakan ini ke peran pengguna yang terkait dengan studio Anda.

`AWSDeadlineCloud-UserAccessJobs`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeadlineCloud-UserAccessJobs` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 April 2024, 17:05 UTC
- Waktu teredit: 07 Oktober 2024, 18:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessJobs`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob",
        "deadline:DisassociateMemberFromJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
```

```
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
        "deadline:UpdateStep",
        "deadline:UpdateTask"
      ],
      "Resource" : [
        "*"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
        }
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:GetJob",
        "deadline:GetJobTemplate",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetTask",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListTasks",
        "deadline:SearchSteps",
        "deadline:SearchTasks"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobs"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDeadlineCloud-UserAccessQueues

Deskripsi: Menyediakan akses workstation pengguna ke antrian Dead AWS line Cloud dengan Read-Only izin terbatas untuk memanggil layanan lain yang diperlukan. Lampirkan kebijakan ini ke peran pengguna yang terkait dengan studio Anda.

`AWSDeadlineCloud-UserAccessQueues`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeadlineCloud-UserAccessQueues` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 01 April 2024, 17:10 UTC
- Waktu teredit: 07 Oktober 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessQueues`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue"
      ],
```

```
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
```

```
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobMembers",
        "deadline:ListQueueMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
        "deadline:UpdateStep",
        "deadline:UpdateTask"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "OwnerManagerContributorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeQueueRoleForUser",
        "deadline:CreateJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR"
          ]
        }
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeQueueRoleForRead",
        "deadline:GetJob",
        "deadline:GetJobTemplate",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListStepConsumers",
```

```
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListStorageProfilesForQueue",
        "deadline:ListTasks",
        "deadline:SearchJobs",
        "deadline:SearchSteps",
        "deadline:SearchTasks"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobs",
        "deadline:ListQueues"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDeadlineCloud-WorkerHost

Deskripsi: Menyediakan akses AWS bagi host pekerja Deadline Cloud untuk bergabung dengan armada di peternakan.

`AWSDeadlineCloud-WorkerHost`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeadlineCloud-WorkerHost` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 April 2024, 17:28 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-WorkerHost`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "JoinFleetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:CreateWorker",
        "deadline:AssumeFleetRoleForWorker"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "TagWorkerPermission",
      "Effect" : "Allow",
      "Action" : [
        "deadline:TagResource"
      ],
      "Resource" : "arn:aws:deadline:*:*:farm/*/fleet/*/worker/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}",
          "deadline:CalledAction" : "CreateWorker"
        }
      }
    },
    {
      "Sid" : "ListFleetTagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListTagsForResource"
      ],
      "Resource" : "arn:aws:deadline:*:*:farm/*/fleet/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}",
          "deadline:CalledAction" : "CreateWorker"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDeepLensLambdaFunctionAccessPolicy

Deskripsi: Kebijakan ini menentukan izin yang diperlukan oleh DeepLens fungsi lambda Administratif yang berjalan di perangkat DeepLens

`AWSDeepLensLambdaFunctionAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeepLensLambdaFunctionAccessPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2017, 15:47 UTC
- Waktu teredit: 11 Juni 2019, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepLensS3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::deeplens*/*",
        "arn:aws:s3:::deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensGreenGrassCloudWatchAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/greengrass/*"
    },
    {
      "Sid" : "DeepLensAccess",
      "Effect" : "Allow",
      "Action" : [
        "deeplens:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensKinesisVideoAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:DescribeStream",
```

```
        "kinesisvideo:CreateStream",
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDeepLensServiceRolePolicy

Deskripsi: Mem AWS DeepLens berikan akses ke Layanan AWS, sumber daya, dan peran yang dibutuhkan oleh DeepLens dan dependensinya termasuk IoT, S3, GreenGrass dan AWS Lambda.

`AWSDeepLensServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeepLensServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 29 November 2017, 15:46 UTC
- Waktu teredit: 25 September 2019, 19.25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepLensIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing",
        "iot:DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensIoTCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot:DeleteCertificate",
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/deeplens*",
        "arn:aws:iot:*:*:cert/*"
      ]
```

```
    },
    {
      "Sid" : "DeepLensIoTCreateCertificateAndPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy",
        "iot:CreatePolicyVersion"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensIoTAttachCertificatePolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/deeplens*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "DeepLensIoTDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:GetThingShadow",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensIoTEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "DeepLensAccess",
      "Effect" : "Allow",
      "Action" : [
        "deeplens:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensS3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteBucket",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensCreateS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensIAMPassRoleAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "greengrass.amazonaws.com",
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DeepLensIAMLambdaPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSDeepLens*",
        "arn:aws:iam::*:role/service-role/AWSDeepLens*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DeepLensGreenGrassAccess",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:AssociateRoleToGroup",
        "greengrass:AssociateServiceRoleToAccount",
        "greengrass:CreateResourceDefinition",
        "greengrass:CreateResourceDefinitionVersion",
        "greengrass:CreateCoreDefinition",
        "greengrass:CreateCoreDefinitionVersion",
        "greengrass:CreateDeployment",
        "greengrass:CreateFunctionDefinition",
```

```
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:CreateGroup",
        "greengrass:CreateGroupCertificateAuthority",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateLoggerDefinition",
        "greengrass:CreateLoggerDefinitionVersion",
        "greengrass:CreateSubscriptionDefinition",
        "greengrass:CreateSubscriptionDefinitionVersion",
        "greengrass:DeleteCoreDefinition",
        "greengrass:DeleteFunctionDefinition",
        "greengrass:DeleteGroup",
        "greengrass:DeleteLoggerDefinition",
        "greengrass:DeleteSubscriptionDefinition",
        "greengrass:DisassociateRoleFromGroup",
        "greengrass:DisassociateServiceRoleFromAccount",
        "greengrass:GetAssociatedRole",
        "greengrass:GetConnectivityInfo",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetDeviceDefinition",
        "greengrass:GetDeviceDefinitionVersion",
        "greengrass:GetFunctionDefinition",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupCertificateAuthority",
        "greengrass:GetGroupCertificateConfiguration",
        "greengrass:GetGroupVersion",
        "greengrass:GetLoggerDefinition",
        "greengrass:GetLoggerDefinitionVersion",
        "greengrass:GetResourceDefinition",
        "greengrass:GetServiceRoleForAccount",
        "greengrass:GetSubscriptionDefinition",
        "greengrass:GetSubscriptionDefinitionVersion",
        "greengrass:ListCoreDefinitionVersions",
        "greengrass:ListCoreDefinitions",
        "greengrass:ListDeployments",
        "greengrass:ListDeviceDefinitionVersions",
        "greengrass:ListDeviceDefinitions",
        "greengrass:ListFunctionDefinitionVersions",
        "greengrass:ListFunctionDefinitions",
        "greengrass:ListGroupCertificateAuthorities",
        "greengrass:ListGroupVersions",
        "greengrass:ListGroups",
```

```
        "greengrass:ListLoggerDefinitionVersions",
        "greengrass:ListLoggerDefinitions",
        "greengrass:ListSubscriptionDefinitionVersions",
        "greengrass:ListSubscriptionDefinitions",
        "greengrass:ResetDeployments",
        "greengrass:UpdateConnectivityInfo",
        "greengrass:UpdateCoreDefinition",
        "greengrass:UpdateDeviceDefinition",
        "greengrass:UpdateFunctionDefinition",
        "greengrass:UpdateGroup",
        "greengrass:UpdateGroupCertificateConfiguration",
        "greengrass:UpdateLoggerDefinition",
        "greengrass:UpdateSubscriptionDefinition",
        "greengrass:UpdateResourceDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensLambdaAdminFunctionAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction",
        "lambda:PublishVersion",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensLambdaUsersFunctionAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
```

```
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*"
      ]
    },
    {
      "Sid" : "DeepLensSageMakerWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:StopTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensSageMakerReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
      ]
    },
    {
      "Sid" : "DeepLensKinesisVideoStreamAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:CreateStream",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:DeleteStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/deeplens*/*"
      ]
    },
    {
      "Sid" : "DeepLensKinesisVideoEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kinesisvideo:GetDataEndpoint"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDeepRacerAccountAdminAccess

Deskripsi: akses DeepRacer admin ke semua tindakan termasuk beralih antara mode multiuser dan pengguna tunggal.

`AWSDeepRacerAccountAdminAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeepRacerAccountAdminAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Oktober 2021, 01:27 UTC
- Waktu teredit: 28 Oktober 2021, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepRacerAdminAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDeepRacerCloudFormationAccessPolicy

Deskripsi: Memungkinkan CloudFormation untuk membuat dan mengelola tum AWS pukan dan sumber daya atas nama Anda.

`AWSDeepRacerCloudFormationAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeepRacerCloudFormationAccessPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Februari 2019, 21:59 UTC
- Waktu teredit: 14 Juni 2019, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
```

```
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpoints",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DetachInternetGateway",
        "ec2:DisassociateRouteTable",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/AWSDeepRacerLambdaAccessRole",
      "Condition" : {
        "StringLikeIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:GetFunction",
        "lambda:DeleteFunction",
        "lambda:TagResource",
        "lambda:UpdateFunctionCode"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*DeepRacer*",
        "arn:aws:lambda:*:*:function:*Deepracer*",
        "arn:aws:lambda:*:*:function:*deepracer*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:DeleteBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "robomaker:CreateSimulationApplication",
        "robomaker:CreateSimulationApplicationVersion",
        "robomaker:DeleteSimulationApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:ListSimulationApplications",
        "robomaker:TagResource",
        "robomaker:UpdateSimulationApplication"
      ],
      "Resource" : [
        "arn:aws:robomaker:*:*:/createSimulationApplication",
        "arn:aws:robomaker:*:*:simulation-application/deepracer*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDeepRacerDefaultMultiUserAccess

Deskripsi: DeepRacer MultiUser Akses pengguna default untuk menggunakan deepracer dalam mode multi-pengguna

`AWSDeepRacerDefaultMultiUserAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeepRacerDefaultMultiUserAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Oktober 2021, 01:27 UTC

- Waktu teredit: 28 Oktober 2021, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:Add*",
        "deepracer:Remove*",
        "deepracer:Create*",
        "deepracer:Perform*",
        "deepracer:Clone*",
        "deepracer:Get*",
        "deepracer:List*",
        "deepracer:Edit*",
        "deepracer:Start*",
        "deepracer:Set*",
        "deepracer:Update*",
        "deepracer:Delete*",
        "deepracer:Stop*",
        "deepracer:Import*",
        "deepracer:Tag*",
        "deepracer:Untag*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
```

```
          "deepracer:UserToken" : "false"
        },
        "Bool" : {
          "deepracer:MultiUser" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:GetAccountConfig",
        "deepracer:GetTrack",
        "deepracer:ListTracks",
        "deepracer:TestRewardFunction"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "deepracer:Admin*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDeepRacerFullAccess

Deskripsi: Menyediakan akses penuh ke AWS DeepRacer. Juga menyediakan akses tertentu ke layanan terkait (misalnya, S3).

`AWSDeepRacerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeepRacerFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Oktober 2020, 22:03 UTC
- Waktu teredit: 05 Oktober 2020, 22:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*",
        "arn:aws:s3:::dr-*",
        "arn:aws:s3:::*DeepRacer*/*",
        "arn:aws:s3:::*Deepracer*/*",
        "arn:aws:s3:::*deepracer*/*",
        "arn:aws:s3:::dr-*/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDeepRacerRoboMakerAccessPolicy

Deskripsi: Memungkinkan RoboMaker untuk membuat sumber daya yang diperlukan dan menelepon AWS layanan atas nama Anda.

`AWSDeepRacerRoboMakerAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeepRacerRoboMakerAccessPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Februari 2019, 21:59 UTC
- Waktu teredit: 28 Februari 2019, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "robomaker:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/robomaker/SimulationJobs",
        "arn:aws:logs:*:*:log-group:/aws/robomaker/SimulationJobs:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*",
        "arn:aws:s3:::dr-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/DeepRacer" : "true"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:CreateStream",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia",
        "kinesisvideo:TagStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/dr-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDeepRacerServiceRolePolicy

Deskripsi: Memungkinkan DeepRacer untuk membuat sumber daya yang diperlukan dan menelepon AWS layanan atas nama Anda.

`AWSDeepRacerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeepRacerServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 28 Februari 2019, 21:58 UTC
- Waktu teredit: 12 Juni 2019, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "robomaker:*",
        "sagemaker:*",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackResource",
```

```
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DetectStackDrift",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:DescribeStackResourceDrifts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "robomaker.amazonaws.com"
        }
      },
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSDeepRacer*",
        "arn:aws:iam::*:role/service-role/AWSDeepRacer*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
```

```
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*DeepRacer*",
        "arn:aws:lambda:*:*:function:*Deepracer*",
        "arn:aws:lambda:*:*:function:*deepracer*",
        "arn:aws:lambda:*:*:function:*dr-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutBucketPolicy",
        "s3:GetBucketAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*",
        "arn:aws:s3:::dr-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/DeepRacer" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "kinesisvideo:CreateStream",
        "kinesisvideo:DeleteStream",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:GetHLSStreamingSessionURL",
        "kinesisvideo:GetMedia",
        "kinesisvideo:PutMedia",
        "kinesisvideo:TagStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/dr-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDenyAll

Deskripsi: Tolak semua akses.

`AWSDenyAll`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDenyAll` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Mei 2019, 22:36 UTC
- Waktu teredit: 18 Desember 2023, 16:42 UTC

- ARN: `arn:aws:iam::aws:policy/AWSDenyAll`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DenyAll",
      "Effect" : "Deny",
      "Action" : [
        "*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDeviceFarmFullAccess

Deskripsi: Menyediakan akses penuh ke semua operasi AWS Device Farm.

`AWSDeviceFarmFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDeviceFarmFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: Juli 13, 2015, 16:37 UTC
- Waktu teredit: 13 Juli 2015, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "devicefarm:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDeviceFarmServiceRolePolicy

Deskripsi: Berikan izin ke AWS Device Farm untuk memanggil API Jaringan EC2 atas nama Anda.

`AWSDeviceFarmServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 20 September 2022, 21:02 UTC
- Waktu teredit: 20 September 2022, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSDeviceFarmManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDeviceFarmTestGridServiceRolePolicy

Deskripsi: Berikan izin ke AWS Device Farm untuk memanggil API EC2 atas nama Anda.

`AWSDeviceFarmTestGridServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 26 Mei 2021, 22:01 UTC
- Waktu teredit: 26 Mei 2021, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSDeviceFarmManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDirectConnectFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Direct Connect melalui Konsol Manajemen AWS.

`AWSDirectConnectFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDirectConnectFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 30 April 2019, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDirectConnectReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke AWS Direct Connect melalui Konsol Manajemen AWS.

`AWSDirectConnectReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDirectConnectReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 18 Mei 2020, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "directconnect:Describe*",
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDirectConnectServiceRolePolicy

Deskripsi: Memberikan izin AWS Direct Connect untuk membuat dan mengelola AWS sumber daya atas nama Anda.

`AWSDirectConnectServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 14 Januari 2021, 18:35 UTC
- Waktu teredit: 14 Januari 2021, 18.35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*directconnect*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDirectoryServiceDataFullAccess

Deskripsi: Menyediakan akses penuh ke Data Layanan AWS Direktori.

`AWSDirectoryServiceDataFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDirectoryServiceDataFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 September 2024, 21:45 UTC
- Waktu teredit: 18 September 2024, 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceDataFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSDataFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ds:AccessDSData",
        "ds-data:AddGroupMember",
        "ds-data:CreateGroup",
        "ds-data:CreateUser",
        "ds-data:DeleteGroup",
        "ds-data:DeleteUser",
        "ds-data:DescribeGroup",
        "ds-data:DescribeUser",
        "ds-data:DisableUser",
        "ds-data:ListGroupMembers",
        "ds-data:ListGroups",
```

```
        "ds-data:ListGroupsForMember",
        "ds-data:ListUsers",
        "ds-data:RemoveGroupMember",
        "ds-data:SearchGroups",
        "ds-data:SearchUsers",
        "ds-data:UpdateGroup",
        "ds-data:UpdateUser"
      ],
      "Resource" : [
        "arn:aws:ds:*:*:directory/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDirectoryServiceDataReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke Data Layanan AWS Direktori

`AWSDirectoryServiceDataReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDirectoryServiceDataReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 September 2024, 22:00 UTC
- Waktu teredit: 18 September 2024, 22:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceDataReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSDataReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ds:AccessDSData",
        "ds-data:DescribeGroup",
        "ds-data:DescribeUser",
        "ds-data:ListGroupMembers",
        "ds-data:ListGroups",
        "ds-data:ListGroupsForMember",
        "ds-data:ListUsers",
        "ds-data:SearchGroups",
        "ds-data:SearchUsers"
      ],
      "Resource" : [
        "arn:aws:ds:*:*:directory/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDirectoryServiceFullAccess

Deskripsi: Menyediakan akses penuh ke Layanan AWS Direktori.

`AWSDirectoryServiceFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDirectoryServiceFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 02 April 2024, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DirectoryServiceFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ds:*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
```

```
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DescribeSecurityGroups",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "iam:ListRoles",
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DirectoryServiceEventTopic",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:DirectoryMonitoring*"
    },
    {
      "Sid" : "DirectoryServiceOrganizations",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "organizations:ServicePrincipal" : "ds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DirectoryServiceTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDirectoryServiceReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Layanan AWS Direktori.

`AWSDirectoryServiceReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDirectoryServiceReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 25 September 2018, 21:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:Check*",
        "ds:Describe*",
        "ds:Get*",
        "ds:List*",
        "ds:Verify*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "sns:ListTopics",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDirectoryServiceServiceRolePolicy

Deskripsi: Kebijakan untuk Peran Tertaut Layanan Direktori

`AWSDirectoryServiceServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 11 Juli 2025, 00:22 UTC
- Waktu teredit: 11 Juli 2025, 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectoryServiceServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SSMSendCommandPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunPowerShellScript",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "EC2DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDiscoveryContinuousExportFirehosePolicy

Deskripsi: Menyediakan akses tulis ke AWS sumber daya yang diperlukan untuk AWS Discovery Continuous Export

`AWSDiscoveryContinuousExportFirehosePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDiscoveryContinuousExportFirehosePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Agustus 2018, 18:29 UTC
- Waktu teredit: 08 Juni 2021, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTableVersions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-application-discovery-service-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/firehose:log-
stream:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDMSFleetAdvisorServiceRolePolicy

Deskripsi: Mengizinkan Penasihat Armada DMS mengelola CloudWatch metrik atas nama Anda.

`AWSDMSFleetAdvisorServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 06 Maret 2023, 09:10 UTC
- Waktu teredit: 06 Maret 2023, 09:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSFleetAdvisorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/DMS/FleetAdvisor"
```

```
      }
    }
  }
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSDMSServerlessServiceRolePolicy

Deskripsi: Mem AWS berikan izin Tanpa Server DMS untuk membuat dan mengelola sumber daya DMS di akun Anda atas nama Anda

`AWSDMSServerlessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 18 Mei 2023, 20:28 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "id0",
      "Effect" : "Allow",
      "Action" : [
        "dms:CreateReplicationInstance",
        "dms:CreateReplicationTask"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dms:req-tag/ResourceCreatedBy" : "DMSServerless"
        }
      }
    },
    {
      "Sid" : "id1",
      "Effect" : "Allow",
      "Action" : [
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "id2",
      "Effect" : "Allow",
      "Action" : [
        "dms:StartReplicationTask",
        "dms:StopReplicationTask",
        "dms:ModifyReplicationTask",
        "dms:DeleteReplicationTask",
        "dms:ModifyReplicationInstance",
        "dms:DeleteReplicationInstance"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:rep:*",
        "arn:aws:dms:*:*:task:*"
      ],
```

```
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/ResourceCreatedBy" : "DMSServerless"
        }
      }
    },
    {
      "Sid" : "id3",
      "Effect" : "Allow",
      "Action" : [
        "dms:TestConnection",
        "dms:DeleteConnection"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:rep:*",
        "arn:aws:dms:*:*:endpoint:*"
      ]
    },
    {
      "Sid" : "id4",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:PutObjectTagging"
      ],
      "Resource" : [
        "arn:aws:s3:::dms-serverless-premigration-results-*",
        "arn:aws:s3:::dms-premigration-results-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "id5",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:GetBucketLocation",
```

```
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::dms-serverless-premigration-results-*",
        "arn:aws:s3:::dms-premigration-results-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "id6",
      "Effect" : "Allow",
      "Action" : [
        "dms:StartReplicationTaskAssessmentRun"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:task:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSEC2CapacityManagerServiceRolePolicy

Deskripsi: Mengizinkan Manajer Kapasitas EC2 mengelola sumber daya kapasitas dan mengintegrasikan dengan AWS Organisasi atas nama Anda.

`AWSEC2CapacityManagerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 09 Oktober 2025, 22:04 UTC
- Waktu teredit: 09 Oktober 2025, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityManagerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOrganizationsDefaultReadActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrganizationsListDelegatedAdministratorsAction",
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "ec2.capacitymanager.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSEC2CapacityReservationFleetRolePolicy

Deskripsi: Mengizinkan layanan EC2 CapacityReservation Armada untuk mengelola Reservasi Kapasitas

`AWSEC2CapacityReservationFleetRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 29 September 2021, 14:43 UTC
- Waktu teredit: 03 Maret 2025, 23:22 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateCapacityReservation",
        "ec2:CancelCapacityReservation",
        "ec2:ModifyCapacityReservation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:CapacityReservationFleet" : "arn:aws:ec2:*:*:capacity-reservation-fleet/
crf-*"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateCapacityReservation"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSEC2FleetServiceRolePolicy

Deskripsi: Mengizinkan EC2 Fleet meluncurkan dan mengelola instans.

`AWSEC2FleetServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 21 Maret 2018, 00:08 UTC
- Waktu teredit: 04 Mei 2020, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2SpotManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:spot-instances-request/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2:fleet-id" : "*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSEC2SpotFleetServiceRolePolicy

Deskripsi: Memungkinkan EC2 Spot Fleet meluncurkan dan mengelola instans armada spot

`AWSEC2SpotFleetServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 23 Oktober 2017, 19:13 UTC
- Waktu teredit: 16 Maret 2020, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:spot-instances-request/*",
        "arn:aws:ec2:*:*:spot-fleet-request/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:*/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSEC2SpotServiceRolePolicy

Deskripsi: Mengizinkan EC2 Spot meluncurkan dan mengelola instans spot

`AWSEC2SpotServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 18 September 2017, 18:51 UTC
- Waktu teredit: 12 Desember 2018, 00:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "ec2:InstanceMarketType" : "spot"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSEC2SqlHaInstancePolicy

Deskripsi: Izin instans Amazon EC2 untuk mengizinkan layanan EC2 SQL High Availability mendeteksi status ketersediaan tinggi instans melalui profil instans EC2.

`AWSEC2SqlHaInstancePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSEC2SqlHaInstancePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 November 2025, 01:49 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEC2SqlHaInstancePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/SqlHaMonitored" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSEc2SqlHa" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSEC2SqlHaServiceRolePolicy

Deskripsi: Izin layanan Ketersediaan Tinggi EC2 SQL untuk mendeteksi instans standby/passive

`AWSEC2SqlHaServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 13 November 2025, 01:34 UTC
- Waktu teredit: 13 November 2025, 01:34 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SqlHaServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSSMSendCommandToTaggedInstances",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/SqlHaMonitored" : "true"
        }
      }
    },
    {
      "Sid" : "AllowSSMSendCommandOfOwnedDoc",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-DetectSqlHa*"
      ]
    },
    {
      "Sid" : "AllowSSMNonMutating",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
```

```
        "ssm:GetCommandInvocation",
        "ssm:ListCommands",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2NonMutating",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEventsMutateManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:PutRule",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ec2sqlha.amazonaws.com",
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      },
      "Resource" : "arn:aws:events:*:*:rule/AWSEC2SqlHa*"
    },
    {
      "Sid" : "AllowEventsNonMutatingManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:ListTargetsByRule",
        "events:DescribeRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AWSEC2SqlHa*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSEC2VssRestorePolicy

Deskripsi: Memberikan izin Amazon EC2 dan AWS SSM untuk memulihkan database SQL Server dari snapshot konsisten aplikasi yang dibuat oleh VSS. AWS

`AWSEC2VssRestorePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSEC2VssRestorePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Maret 2026, 23:12 UTC
- Waktu teredit: 25 Maret 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEC2VssRestorePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "CreateVolumeAccessVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AwsVssConfig" : "*"
        },
        "ArnLike" : {
          "ec2:ParentSnapshot" : "arn:aws:ec2:*:*:snapshot/*"
        }
      }
    },
    {
      "Sid" : "CreateVolumeAccessSnapshot",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/AwsVssConfig" : "*"
        }
      }
    },
    {
      "Sid" : "CreateVolumeWithTagging",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVolume"
        }
      }
    },
    {
      "Sid" : "AttachVolumeAccessVolume",
      "Effect" : "Allow",
      "Action" : "ec2:AttachVolume",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/AwsVssConfig" : "*"
```

```
        }
      }
    },
    {
      "Sid" : "AttachVolumeAccessInstance",
      "Effect" : "Allow",
      "Action" : "ec2:AttachVolume",
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DescribeVolumes",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeVolumes",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeSnapshots",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSnapshots",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstanceAttribute",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstanceAttribute",
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "SsmAutomationRead",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SsmRunCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetDocument"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:document/AWSEC2-PrepareVssRestore",
        "arn:aws:ssm:*:*:document/AWSEC2-RunVssRestoreForSqlDatabase"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSEC2VssSnapshotPolicy

Deskripsi: Kebijakan ini dilampirkan ke peran IAM yang dilampirkan ke Instans Windows Amazon EC2 Anda untuk mengaktifkan solusi Amazon EC2 VSS untuk membuat dan menambahkan tag ke Amazon Machine Images (AMI) dan Snapshots EBS.

`AWSEC2VssSnapshotPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSEC2VssSnapshotPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Maret 2024, 16:32 UTC
- Waktu teredit: 20 November 2024, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEC2VssSnapshotPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstanceInfo",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:SourceInstanceARN" : "arn:aws:ec2:*:*:instance/${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AwsVssConfig" : "*"
        }
      }
    },
```

```
    {
      "Sid" : "CreateSnapshotsAccessInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:SourceInstanceARN" : "arn:aws:ec2:*:*:instance/${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsAccessVolume",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "CreateImageWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AwsVssConfig" : "*"
        }
      }
    },
    {
      "Sid" : "CreateImageAccessInstance",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:SourceInstanceARN" : "arn:aws:ec2:*:*:instance/${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnResourceCreation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateImage",
            "CreateSnapshots"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsAfterResourceCreation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/AwsVssConfig" : "*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AppConsistent",
```

```
            "Device"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeImagesAndSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSECRPullThroughCache_ServiceRolePolicy

Deskripsi: Mengaktifkan akses ke AWS layanan dan sumber daya yang digunakan atau dikelola oleh AWS penarikan cache ECR

`AWSECRPullThroughCache_ServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran

- Waktu pembuatan: 26 November 2021, 21:51 UTC
- Waktu teredit: 12 Mei 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECR",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:PutImage",
        "ecr:BatchGetImage",
        "ecr:BatchImportUpstreamImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetImageCopyStatus"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "SecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecr-pullthroughcache/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticBeanstalkCustomPlatformforEC2Role

Deskripsi: Berikan izin instance di lingkungan pembuat platform kustom Anda untuk meluncurkan instans EC2, membuat snapshot EBS dan AMI, melakukan streaming log ke Amazon Logs CloudWatch , dan menyimpan artefak di Amazon S3.

`AWSElasticBeanstalkCustomPlatformforEC2Role`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkCustomPlatformforEC2Role` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Februari 2017, 22:50 UTC
- Waktu teredit: 21 Februari 2017, 22:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Access",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CopyImage",
        "ec2:CreateImage",
        "ec2:CreateKeypair",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteKeypair",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeleteVolume",
        "ec2:DeregisterImage",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume",
        "ec2:GetPasswordData",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
```

```
        "ec2:ModifySnapshotAttribute",
        "ec2:RegisterImage",
        "ec2:RunInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "BucketAccess",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "CloudWatchLogsAccess",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/platform/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticBeanstalkEKSImageBuild

Deskripsi: Izin yang diperlukan oleh Elastic Beanstalk untuk membuat gambar kontainer atas nama pelanggan.

`AWSElasticBeanstalkEKSImageBuild`dadalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkEKSImageBuild` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Juli 2026, 21:27 UTC
- Waktu teredit: 02 Juli 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkEKSImageBuild`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3SourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : [
```

```
        "arn:aws:s3:::*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ECRAuthToken",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ECRPublicAuthToken",
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken",
        "sts:GetServiceBearerToken"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ECRRepositoryAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:PutImage",
        "ecr:InitiateLayerUpload",
```

```
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/elasticbeanstalk-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/elasticbeanstalk-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticBeanstalkEKSObservability

Deskripsi: Izin pengamatan untuk lingkungan Elastic Beanstalk yang berjalan di cluster Layanan Kubernetes Elastic

`AWSElasticBeanstalkEKSObservability`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkEKSObservability` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Juli 2026, 21:27 UTC
- Waktu teredit: 02 Juli 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkEKSObservability`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FluentBitS3Plugin",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-logs-*",
        "arn:aws:s3:::elasticbeanstalk-logs-*/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "APSCreateWorkspace",
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateWorkspace",
        "aps:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "ElasticBeanstalk",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "APSManageWorkspace",
      "Effect" : "Allow",
      "Action" : [
        "aps:DeleteWorkspace",
        "aps:Describe*"
      ],
      "Resource" : "arn:aws:aps:*:*:workspace/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "ElasticBeanstalk",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "APSRemoteWrite",
      "Effect" : "Allow",
      "Action" : [
        "aps:RemoteWrite"
      ],
      "Resource" : "arn:aws:aps:*:*:workspace/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/CreatedBy" : "ElasticBeanstalk",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticBeanstalkEKSTagging

Deskripsi: Izin diperlukan untuk melewati tag ke sumber daya yang dibuat oleh Pengontrol EKS

`AWSElasticBeanstalkEKSTagging`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkEKSTagging` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Juli 2026, 21:27 UTC
- Waktu teredit: 02 Juli 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkEKSTagging`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Compute",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances",
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "StringLike" : {
          "aws:RequestTag/eks:kubernetes-node-class-name" : "*",
          "aws:RequestTag/eks:kubernetes-node-pool-name" : "*"
        }
      }
    },
    {
      "Sid" : "Storage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Sid" : "Networking",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "StringLike" : {
          "aws:RequestTag/eks:kubernetes-cni-node-name" : "*"
        }
      }
    },
    {
      "Sid" : "LoadBalancer",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateRule",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Sid" : "ShieldProtection",
      "Effect" : "Allow",
      "Action" : [
        "shield:CreateProtection"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Sid" : "ShieldTagResource",
      "Effect" : "Allow",
      "Action" : [
        "shield:TagResource"
      ],
      "Resource" : "arn:aws:shield::*:protection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticBeanstalkEnhancedHealth

Deskripsi: Kebijakan Layanan AWS Elastic Beanstalk untuk sistem Pemantauan Kesehatan

`AWSElasticBeanstalkEnhancedHealth`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkEnhancedHealth` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 08 Februari 2016, 23:17 UTC
- Waktu teredit: 09 April 2018, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:GetConsoleOutput",
        "ec2:AssociateAddress",
        "ec2:DescribeAddresses",
        "ec2:DescribeSecurityGroups",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
```

```
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeNotificationConfigurations",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*:log-stream:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticBeanstalkMaintenance

Deskripsi: Kebijakan Peran Layanan AWS Elastic Beanstalk yang memberikan izin terbatas untuk memperbarui sumber daya atas nama Anda untuk tujuan pemeliharaan.

`AWSElasticBeanstalkMaintenance`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 11 Januari 2019, 23:22 UTC
- Waktu teredit: 29 April 2024, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationChangeSetOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DescribeStacks",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
```

```
      "Sid" : "AllowElasticBeanstalkStacksUpdateExecuteSuccessfully",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

Deskripsi: Kebijakan ini untuk peran layanan AWS Elastic Beanstalk yang digunakan untuk melakukan pembaruan terkelola lingkungan Elastic Beanstalk. Kebijakan ini tidak boleh dilampirkan ke pengguna atau peran lain. Kebijakan ini memberikan izin luas untuk membuat dan mengelola sumber daya di sejumlah AWS layanan termasuk AutoScaling, EC2, ECS, Elastic Load Balancing dan. CloudFormation Kebijakan ini juga memungkinkan penerusan peran IAM apa pun yang dapat digunakan dengan layanan tersebut.

`AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Maret 2021, 22:18 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticBeanstalkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticbeanstalk:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScheduledActions",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "logs:DescribeLogGroups",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeOrderableDBInstanceOptions",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2BroadOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
```

```
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteSecurityGroup",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2RunInstancesOperationPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "EC2TerminateInstancesOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
          ]
        }
      }
    },
    {
      "Sid" : "ECSBroadOperationPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:DescribeClusters",
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECSDeleteClusterOperationPermissions",
      "Effect" : "Allow",
      "Action" : "ecs:DeleteCluster",
      "Resource" : "arn:aws:ecs:*:*:cluster/awseb-*"
    },
    {
      "Sid" : "ASGOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:DeletePolicy",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:ResumeProcesses",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:SuspendProcesses",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
```

```
    {
      "Sid" : "CFNOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "ELBOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/eb-*/*"
      ]
    },
    {
      "Sid" : "CWLogsOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
```

```
    {
      "Sid" : "S3ObjectOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
    {
      "Sid" : "S3BucketOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "SNSOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "sns:Subscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
    },
    {
      "Sid" : "SQSOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl"
      ],
```

```
      "Resource" : [
        "arn:aws:sqs:*:*:awseb-e-*",
        "arn:aws:sqs:*:*:eb-*"
      ]
    },
    {
      "Sid" : "CWPutMetricAlarmOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:awseb-*",
        "arn:aws:cloudwatch:*:*:alarm:eb-*"
      ]
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchTemplateTagPropagationPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:createTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "RunInstances",
            "AllocateAddress"
          ]
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

Deskripsi: Kebijakan Peran Layanan AWS Elastic Beanstalk yang memberikan izin terbatas untuk pembaruan terkelola.

`AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 21 November 2019, 22:35 UTC
- Waktu teredit: 13 Maret 2026, 16:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SingleInstanceAPIs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:releaseAddress",
        "ec2:allocateAddress",
        "ec2:DisassociateAddress",
        "ec2:AssociateAddress"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RegisterTaskDefinition",
```

```
        "ecs:DeRegisterTaskDefinition",
        "ecs:List*",
        "ecs:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ElasticBeanstalkAPIs",
      "Effect" : "Allow",
      "Action" : [
        "elasticbeanstalk:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyAPIs",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:Describe*",
        "cloudformation:List*",
        "ec2:Describe*",
        "autoscaling:Describe*",
        "elasticloadbalancing:Describe*",
        "logs:DescribeLogGroups",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ASG",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:PutNotificationConfiguration",
```

```
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
    {
      "Sid" : "CFN",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CancelUpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:UpdateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-e-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
```

```
        ]
      }
    }
  },
  {
    "Sid" : "S3Obj",
    "Effect" : "Allow",
    "Action" : [
      "s3:DeleteObject",
      "s3:GetObject",
      "s3:GetObjectAcl",
      "s3:GetObjectVersion",
      "s3:GetObjectVersionAcl",
      "s3:PutObject",
      "s3:PutObjectAcl",
      "s3:PutObjectVersionAcl"
    ],
    "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
  },
  {
    "Sid" : "S3Bucket",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation",
      "s3:GetBucketPolicy",
      "s3:ListBucket",
      "s3:PutBucketPolicy"
    ],
    "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
  },
  {
    "Sid" : "CWL",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup",
      "logs:DeleteLogGroup",
      "logs:PutRetentionPolicy"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
  },
  {
    "Sid" : "ELB",
    "Effect" : "Allow",
    "Action" : [
```

```
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeRegisterTargets",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-e-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*"
      ]
    },
    {
      "Sid" : "SNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-Environment-*"
    },
    {
      "Sid" : "EC2LaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*"
    },
    {
      "Sid" : "AllowLaunchTemplateRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "AllowECSTagResource",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "RegisterTaskDefinition"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchTemplateTagPropagationPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:createTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "RunInstances",
            "AllocateAddress"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticBeanstalkMulticontainerDocker

Deskripsi: Menyediakan instans di akses lingkungan Docker multicontainer Anda untuk menggunakan Amazon EC2 Container Service untuk mengelola tugas penerapan kontainer.

`AWSElasticBeanstalkMulticontainerDocker`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkMulticontainerDocker` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Februari 2016, 23:15 UTC
- Waktu teredit: 29 April 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecs:Poll",
        "ecs:StartTask",
        "ecs:StopTask",
        "ecs:DiscoverPollEndpoint",
        "ecs:StartTelemetrySession",
        "ecs:RegisterContainerInstance",
        "ecs:DeregisterContainerInstance",
        "ecs:DescribeContainerInstances",
        "ecs:Submit*",
```

```
        "ecs:DescribeTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "RegisterContainerInstance",
            "StartTask"
          ]
        }
      }
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeFoundationModel",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/anthropic.claude-*",
        "arn:aws:bedrock:*::foundation-model/amazon.nova-*"
      ]
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeInferenceProfile",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*anthropic.claude-*",
        "arn:aws:bedrock:*:*:inference-profile/*amazon.nova-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "AIEnvironmentAnalysisReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels",
        "elasticbeanstalk:DescribeEvents",
        "elasticbeanstalk:DescribeEnvironmentHealth"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrock",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticBeanstalkReadOnly

Deskripsi: Memberikan izin baca-saja. Secara eksplisit memungkinkan operator untuk mendapatkan akses langsung untuk mengambil informasi tentang sumber daya yang terkait dengan aplikasi AWS Elastic Beanstalk.

`AWSElasticBeanstalkReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 Januari 2021, 19:02 UTC
- Waktu yang diedit: 19 Mei 2026, 13:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAPIs",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScheduledActions",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
```

```
        "cloudformation:ValidateTemplate",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeSSLPolicies",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListServerCertificates",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribeDBSnapshots",
        "s3:ListAllMyBuckets",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sqs:ListQueues"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "AllowCloudWatchLogsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Sid" : "AllowCloudWatchLogsRead",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*:log-stream:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticBeanstalkRoleCore

Deskripsi: AWSElasticBeanstalkRoleCore (Peran operasi Elastic Beanstalk) Memungkinkan operasi inti dari lingkungan layanan web.

`AWSElasticBeanstalkRoleCore`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkRoleCore` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Juni 2020, 21:48 UTC
- Waktu teredit: 30 April 2024, 00:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/awseb-e-*"
        }
      }
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReleaseAddress",
        "ec2:AllocateAddress",
        "ec2:DisassociateAddress",
        "ec2:AssociateAddress",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroup*",
        "ec2:RevokeSecurityGroup*",
        "ec2:CreateLaunchTemplate*",
        "ec2:DeleteLaunchTemplate*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LTRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "ASG",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:*LoadBalancer*",
```

```
        "autoscaling:*AutoScalingGroup",
        "autoscaling:*LaunchConfiguration",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:*Tags"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*"
      ]
    },
    {
      "Sid" : "ASGPolicy",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DeletePolicy"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EBSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/elasticbeanstalk.amazonaws.com/
AWSServiceRoleForElasticBeanstalk*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticbeanstalk.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "S3Obj",
      "Effect" : "Allow",
      "Action" : [
        "s3:Delete*",
        "s3:Get*",
        "s3:Put*"
      ],
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*/*",
        "arn:aws:s3:::elasticbeanstalk-env-resources-*/*"
      ]
    },
    {
      "Sid" : "S3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucket*",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "CFN",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:UpdateStack",
        "cloudformation:ContinueUpdateRollback",
        "cloudformation:CancelUpdateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/awseb-e-*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
```

```
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:awseb-*"
    },
    {
      "Sid" : "ELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Create*",
        "elasticloadbalancing:Delete*",
        "elasticloadbalancing:Modify*",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeRegisterTargets",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:*Tags",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:SetRulePriorities",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/net/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/awseb-*/*/*/*"
      ]
    },
    {
      "Sid" : "ListAPIs",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudformation:Describe*",
        "logs:Describe*",
        "ec2:Describe*",
        "ecs:Describe*",
        "ecs:List*",
        "elasticloadbalancing:Describe*",
        "rds:Describe*",
        "sns:List*",
        "iam:List*",
```

```
        "acm:Describe*",
        "acm:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/aws-elasticbeanstalk-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticBeanstalkRoleCWL

Deskripsi: (Peran operasi Elastic Beanstalk) Memungkinkan lingkungan untuk mengelola grup CloudWatch log Amazon Logs.

`AWSElasticBeanstalkRoleCWL`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkRoleCWL` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Juni 2020, 21:49 UTC
- Waktu teredit: 05 Juni 2020, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticBeanstalkRoleECS

Deskripsi: (Peran operasi Elastic Beanstalk) Memungkinkan lingkungan Docker multicontainer untuk mengelola cluster Amazon ECS.

`AWSElasticBeanstalkRoleECS`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkRoleECS` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Juni 2020, 21:47 UTC
- Waktu teredit: 23 Maret 2023, 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:DeleteCluster",
        "ecs:RegisterTaskDefinition",
        "ecs:DeRegisterTaskDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticBeanstalkRoleRDS

Deskripsi: (Peran operasi Elastic Beanstalk) Memungkinkan lingkungan untuk mengintegrasikan instance Amazon RDS.

`AWSElasticBeanstalkRoleRDS`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkRoleRDS` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Juni 2020, 21:46 UTC
- Waktu teredit: 05 Juni 2020, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBSecurityGroup",
        "rds:DeleteDBSecurityGroup",
        "rds:AuthorizeDBSecurityGroupIngress",
        "rds:CreateDBInstance",
        "rds:ModifyDBInstance",
```

```
        "rds:DeleteDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:secgrp:awseb-e-*",
        "arn:aws:rds:*:*:db:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticBeanstalkRoleSNS

Deskripsi: (Peran operasi Elastic Beanstalk) Memungkinkan lingkungan untuk mengaktifkan integrasi topik Amazon SNS.

`AWSElasticBeanstalkRoleSNS`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkRoleSNS` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Juni 2020, 21:46 UTC
- Waktu teredit: 05 Juni 2020, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowBeanstalkManageSNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes",
        "sns:DeleteTopic"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
      ]
    },
    {
      "Sid" : "AllowSNSPublish",
      "Effect" : "Allow",
      "Action" : [
        "sns:GetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticBeanstalkRoleWorkerTier

Deskripsi: (Peran operasi Elastic Beanstalk) Mengizinkan tingkat lingkungan pekerja untuk membuat tabel Amazon DynamoDB dan antrian Amazon SQS.

`AWSElasticBeanstalkRoleWorkerTier`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkRoleWorkerTier` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Juni 2020, 21:43 UTC
- Waktu teredit: 05 Juni 2020, 21:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSQS",
      "Effect" : "Allow",
      "Action" : [
        "sqs:TagQueue",
```

```
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:CreateQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:awseb-e-*"
    },
    {
      "Sid" : "AllowDDB",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:TagResource",
        "dynamodb:DescribeTable",
        "dynamodb:DeleteTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/awseb-e-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticBeanstalkService

Deskripsi: Kebijakan ini berada di jalur penghentian. Lihat dokumentasi untuk panduan: Kebijakan peran Layanan Beanstalk https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/iam-servicerole.html. AWS Elastic yang memberikan izin untuk membuat & mengelola sumber daya (yaitu: AutoScaling, EC2, S3,, ELB CloudFormation, dll.) atas nama Anda.

`AWSElasticBeanstalkService`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkService` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 April 2016, 20:27 UTC
- Waktu teredit: 10 Mei 2023, 19:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService`

Versi kebijakan

Versi kebijakan: v17 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "AllowDeleteCloudwatchLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
      ]
```

```
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    },
    {
      "Sid" : "AllowS3OperationsOnElasticBeanstalkBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:*"
      ],
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "AllowLaunchTemplateRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "AllowELBAddTags",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateLoadBalancer"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOperations",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DetachInstances",
        "autoscaling:DeletePolicy",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:ResumeProcesses",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:SuspendProcesses",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup",
        "cloudwatch:PutMetricAlarm",
        "ec2:AssociateAddress",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
```

```
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeVpcClassicLink",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:TerminateInstances",
        "ecs:CreateCluster",
        "ecs:DeleteCluster",
        "ecs:DescribeClusters",
        "ecs:RegisterTaskDefinition",
        "elasticbeanstalk:*",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "iam:ListRoles",
        "iam:PassRole",
```

```
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogGroups",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeOrderableDBInstanceOptions",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:ListBucket",
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "sns:Subscribe",
        "sns:SetTopicAttributes",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticBeanstalkServiceRolePolicy

Deskripsi: Kebijakan Peran Tertaut Layanan Beanstalk E AWS lastic yang memberikan izin untuk membuat & mengelola sumber daya (yaitu: AutoScaling, EC2, S3,, ELB CloudFormation, dll.) atas nama Anda.

`AWSElasticBeanstalkServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 13 September 2017, 23:46 UTC
- Waktu teredit: 18 Agustus 2026, 17:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationReadOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
```

```
    },
    {
      "Sid" : "AllowOperations",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:PutNotificationConfiguration",
        "ec2:DescribeInstanceStatus",
        "ec2:AssociateAddress",
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "lambda:GetFunction",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowOperationsOnHealthStreamingLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DeleteLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Sid" : "EBEKSGeneralOperations",
      "Effect" : "Allow",
      "Action" : [
```

```
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:DescribeRepositories",
        "ecr:ListTagsForResource",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "iam:GetRole",
        "codebuild:ListProjects",
        "codebuild:BatchGetProjects",
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "elasticbeanstalk:DescribeEvents",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticbeanstalk:DescribeConfigurationSettings"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSDefaultHTTPSCertCreate",
      "Effect" : "Allow",
      "Action" : [
        "acm:RequestCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
```

```
          "aws:RequestTag/elasticbeanstalk:environment-id" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSDefaultHTTPSCertModifyDelete",
      "Effect" : "Allow",
      "Action" : [
        "acm:AddTagsToCertificate",
        "acm:DeleteCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/elasticbeanstalk:environment-id" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSSubnetTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "kubernetes.io/role/elb",
            "kubernetes.io/role/internal-elb"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "EBEKSIamCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:AWSServiceName" : "eks.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EBEKSIamPermissionsImageBuild",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "codebuild.amazonaws.com",
            "eks.amazonaws.com",
            "ec2.amazonaws.com",
            "pods.eks.amazonaws.com",
            "elasticbeanstalk.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EBEKSS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetObjectVersion",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSEKSClusterManagement",
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateCluster",
        "eks:DeleteCluster",
        "eks:DescribeCluster",
        "eks:DescribeUpdate",
        "eks:CreateAccessEntry",
        "eks:DeleteAccessEntry",
        "eks:CreateAddon",
        "eks:CreatePodIdentityAssociation",
        "eks:ListPodIdentityAssociations"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/beanstalk-cluster*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSEKSAddonManagement",
      "Effect" : "Allow",
      "Action" : [
        "eks:DeleteAddon",
        "eks:DescribeAddon",
        "eks:UpdateAddon"
      ],
      "Resource" : "arn:aws:eks:*:*:addon/beanstalk-cluster*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "EBEKSEKSAccessEntryManagement",
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DescribeAccessEntry",
        "eks:ListAssociatedAccessPolicies"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/beanstalk-cluster*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSEKSPodIdentityManagement",
      "Effect" : "Allow",
      "Action" : [
        "eks:DeletePodIdentityAssociation",
        "eks:DescribePodIdentityAssociation",
        "eks:UpdatePodIdentityAssociation"
      ],
      "Resource" : "arn:aws:eks:*:*:podidentityassociation/beanstalk-cluster*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSCodeBuildProjectManagement",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:UpdateProject",
        "codebuild:StartBuild",
        "codebuild:BatchGetBuilds",
        "codebuild:BatchGetProjects"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/elasticbeanstalk-*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSECRRepositoryManagement",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:DescribeRepositories",
        "ecr:DescribeImages",
        "ecr:PutLifecyclePolicy",
        "ecr:TagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/elasticbeanstalk-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSCFNStackManagementImageBuild",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/elasticbeanstalk-*-image-build",
        "arn:aws:cloudformation:*:*:stack/elasticbeanstalk-*-image-build/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSCFNStackManagementClusterSetup",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudformation:UpdateStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/beanstalk-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSAPSCreateWorkspace",
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateWorkspace",
        "aps:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "ElasticBeanstalk",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSAPSManageWorkspace",
      "Effect" : "Allow",
      "Action" : [
        "aps:DeleteWorkspace",
        "aps:Describe*"
      ],
      "Resource" : "arn:aws:aps:*:*:workspace/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "ElasticBeanstalk"
```

```
        }
      }
    },
    {
      "Sid" : "EBEKSAPSRemoteWrite",
      "Effect" : "Allow",
      "Action" : [
        "aps:RemoteWrite"
      ],
      "Resource" : "arn:aws:aps:*:*:workspace/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "ElasticBeanstalk"
        }
      }
    },
    {
      "Sid" : "EBEKSCreateDashboard",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutDashboard",
      "Resource" : "arn:aws:cloudwatch::*:dashboard/ElasticBeanstalk-Observability-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbLoadBalancerWrite",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:SetSecurityGroups",
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbTargetGroupCreate",
```

```
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/elasticbeanstalk:environment-id" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbTargetGroupModifyDelete",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/elasticbeanstalk:environment-id" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbListenerRuleCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateRule",
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*"
      ],
```

```
      "Condition" : {
        "Null" : {
          "aws:RequestTag/elasticbeanstalk:environment-id" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbListenerRuleDelete",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteRule"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/elasticbeanstalk:environment-id" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbEC2CreateSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/elasticbeanstalk:byo-alb-arn" : "false",
          "aws:RequestTag/elasticbeanstalk:managed" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbEC2CreateSecurityGroupVpc",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbEC2CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/elasticbeanstalk:byo-alb-arn" : "false",
          "aws:RequestTag/elasticbeanstalk:managed" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbEC2SecurityGroupEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/elasticbeanstalk:byo-alb-arn" : "false",
          "aws:ResourceTag/elasticbeanstalk:managed" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "ECRTagMutation",
      "Effect" : "Allow",
      "Action" : [
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/elasticbeanstalk:application-name" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CodeBuildTagMutation",
      "Effect" : "Allow",
      "Action" : "codebuild:UpdateProject",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/elasticbeanstalk:application-name" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagMutation",
      "Effect" : "Allow",
      "Action" : [
        "acm:AddTagsToCertificate",
        "acm:RemoveTagsFromCertificate",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:RemoveTags",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/elasticbeanstalk:environment-id" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticBeanstalkWebTier

Deskripsi: Menyediakan akses instance di lingkungan server web Anda untuk mengunggah file log ke Amazon S3.

`AWSElasticBeanstalkWebTier`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkWebTier` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Februari 2016, 23:08 UTC
- Waktu teredit: 29 April 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BucketAccess",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "XRayAccess",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsAccess",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
      ]
    },
    {
      "Sid" : "ElasticBeanstalkHealthAccess",
      "Action" : [
        "elasticbeanstalk:PutInstanceStatistics"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:elasticbeanstalk:*:*:application/*",
        "arn:aws:elasticbeanstalk:*:*:environment/*"
      ]
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeFoundationModel",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/anthropic.claude-*",
        "arn:aws:bedrock:*::foundation-model/amazon.nova-*"
      ]
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeInferenceProfile",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*anthropic.claude-*",
        "arn:aws:bedrock:*:*:inference-profile/*amazon.nova-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AIEnvironmentAnalysisReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels",
        "elasticbeanstalk:DescribeEvents",
```

```
        "elasticbeanstalk:DescribeEnvironmentHealth"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrock",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticBeanstalkWorkerTier

Deskripsi: Menyediakan akses instance di lingkungan pekerja Anda untuk mengunggah file log ke Amazon S3, untuk menggunakan Amazon SQS untuk memantau antrian pekerjaan aplikasi Anda, untuk menggunakan Amazon DynamoDB untuk melakukan pemilihan pemimpin, dan ke Amazon CloudWatch untuk menerbitkan metrik untuk pemantauan kesehatan.

`AWSElasticBeanstalkWorkerTier`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticBeanstalkWorkerTier` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Februari 2016, 23:12 UTC
- Waktu teredit: 29 April 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MetricsAccess",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "XRayAccess",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "QueueAccess",
      "Action" : [
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:ReceiveMessage",
        "sqs:SendMessage"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "BucketAccess",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "DynamoPeriodicTasks",
      "Action" : [
        "dynamodb:BatchGetItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:DeleteItem",
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dynamodb:UpdateItem"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/*-stack-AWSEBWorkerCronLeaderRegistry*"
      ]
    },
    {
      "Sid" : "CloudWatchLogsAccess",
      "Action" : [
```

```
        "logs:PutLogEvents",
        "logs:CreateLogStream"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
      ]
    },
    {
      "Sid" : "ElasticBeanstalkHealthAccess",
      "Action" : [
        "elasticbeanstalk:PutInstanceStatistics"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:elasticbeanstalk:*:*:application/*",
        "arn:aws:elasticbeanstalk:*:*:environment/*"
      ]
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeFoundationModel",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/anthropic.claude-*",
        "arn:aws:bedrock:*::foundation-model/amazon.nova-*"
      ]
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeInferenceProfile",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*anthropic.claude-*",
        "arn:aws:bedrock:*:*:inference-profile/*amazon.nova-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AIEnvironmentAnalysisReadOnly",
```

```
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels",
        "elasticbeanstalk:DescribeEvents",
        "elasticbeanstalk:DescribeEnvironmentHealth"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrock",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticDisasterRecoveryAgentInstallationPolicy

Deskripsi: Kebijakan ini memungkinkan penginstalan Agen AWS Replikasi, yang digunakan dengan AWS Elastic Disaster Recovery (DRS) untuk memulihkan server eksternal. AWS Lampirkan kebijakan ini ke pengguna atau peran IAM yang kredensialnya Anda berikan selama langkah penginstalan Agen AWS Replikasi.

`AWSElasticDisasterRecoveryAgentInstallationPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryAgentInstallationPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 November 2021, 10:37 UTC
- Waktu teredit: 27 November 2023, 12:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryAgentInstallationPolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSAgentInstallationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:CreateSourceServerForDrs",
        "drs:CreateRecoveryInstanceForDrs",
        "drs:DescribeRecoveryInstances",
        "drs:CreateSourceNetwork"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "DRSAgentInstallationPolicy2",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    },
    {
      "Sid" : "DRSAgentInstallationPolicy3",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateRecoveryInstanceForDrs"
        }
      }
    },
    {
      "Sid" : "DRSAgentInstallationPolicy4",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-network/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceNetwork"
        }
      }
    },
    {
      "Sid" : "DRSAgentInstallationPolicy5",
      "Effect" : "Allow",
      "Action" : "drs:IssueAgentCertificateForDrs",
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticDisasterRecoveryAgentPolicy

Deskripsi: Kebijakan ini memungkinkan penggunaan Agen AWS Replikasi, yang digunakan dengan AWS Elastic Disaster Recovery (DRS) untuk memulihkan server sumber ke AWS. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSElasticDisasterRecoveryAgentPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryAgentPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 17 November 2021, 10:32 UTC
- Waktu teredit: 27 November 2023, 13:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSAgentPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs",
        "drs:IssueAgentCertificateForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/${aws:SourceIdentity}"
    },
    {
      "Sid" : "DRSAgentPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticDisasterRecoveryConsoleFullAccess

Deskripsi: Kebijakan ini menyediakan akses penuh ke semua API publik AWS Elastic Disaster Recovery (DRS), serta izin untuk membaca kunci KMS, Manajer Lisensi, Grup Sumber Daya, Elastic Load Balancing, IAM, dan informasi EC2. Lampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSElasticDisasterRecoveryConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 November 2021, 10:46 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeHosts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess4",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ConsoleFullAccess5",
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess6",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess7",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess8",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
```

```
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
```

```
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess16",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "ConsoleFullAccess17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "ConsoleFullAccess18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
```

```
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2:StartInstances",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "ConsoleFullAccess23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess25",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
```

```
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess26",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances"
          ]
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess28",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess29",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess30",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticDisasterRecoveryConsoleFullAccess_v2

Deskripsi: Kebijakan ini menyediakan akses penuh ke semua API publik AWS Elastic Disaster Recovery (AWS DRS), serta semua API publik di AWS layanan lain yang digunakan oleh AWS DRS Console. Lampirkan kebijakan ini ke pengguna atau peran Anda.

`AWSElasticDisasterRecoveryConsoleFullAccess_v2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryConsoleFullAccess_v2` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2023, 13:35 UTC
- Waktu teredit: 18 Juni 2026, 22:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess_v2`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeHosts",
        "ec2:GetInstanceTypesFromInstanceRequirements"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess4",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "ConsoleFullAccess5",
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess6",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess7",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess8",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess9",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess12",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
```

```
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess16",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "ConsoleFullAccess17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
```

```
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2:StartInstances",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "ec2:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "ConsoleFullAccess23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess25",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
```

```
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess26",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "ConsoleFullAccess28",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess29",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess30",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess31",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
```

```
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-CreateImage:$DEFAULT",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateNetworkConnectivity",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyMountedVolumes",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateHttpResponse",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateDiskSpace",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyProcessIsRunning",
        "arn:aws:ssm:*:*:document/AWSMigration-LinuxTimeSyncSetting",
        "arn:aws:ssm:*:*:document/AWSDRS-ValidateNetworkConnectivity",
        "arn:aws:ssm:*:*:document/AWSDRS-VerifyMountedVolumes",
        "arn:aws:ssm:*:*:document/AWSDRS-ValidateHttpResponse",
        "arn:aws:ssm:*:*:document/AWSDRS-ValidateDiskSpace",
        "arn:aws:ssm:*:*:document/AWSDRS-VerifyProcessIsRunning",
        "arn:aws:ssm:*:*:document/AWSDRS-LinuxTimeSyncSetting",
        "arn:aws:ssm:*:*:document/AWSDRS-InstallDRAgentOnInstance",
        "arn:aws:ssm:*:*:document/AWSDRS-VerifyTags",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure",
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess32",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
```

```
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess33",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess34",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess35",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ConsoleFullAccess36",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
```

```
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecovery-*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess37",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess38",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess39",
      "Effect" : "Allow",
      "Action" : "ec2:CreateFleet",
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess40",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateFleet"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess41",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess42",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess43",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "ConsoleFullAccess44",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticDisasterRecoveryConversionServerPolicy

Deskripsi: Kebijakan ini dilampirkan ke peran instans server AWS Elastic Disaster Recovery Conversion. Kebijakan ini memungkinkan Server Konversi Elastic Disaster Recovery (DRS), yang merupakan instans EC2 yang diluncurkan oleh Elastic Disaster Recovery, untuk berkomunikasi dengan layanan DRS. Peran IAM dengan kebijakan ini dilampirkan (sebagai Profil Instans EC2) oleh DRS ke Server Konversi DRS, yang secara otomatis diluncurkan dan dihentikan oleh DRS, bila diperlukan. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda. Server Konversi DRS digunakan oleh Elastic Disaster Recovery ketika pengguna memilih untuk memulihkan server sumber menggunakan konsol DRS, CLI, atau API.

`AWSElasticDisasterRecoveryConversionServerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryConversionServerPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 17 November 2021, 13:42 UTC
- Waktu teredit: 27 November 2023, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryConversionServerPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSConversionServerPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSConversionServerPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetChannelCommandsForDrs",
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

Deskripsi: Kebijakan ini memungkinkan AWS Elastic Disaster Recovery (DRS) mendukung replikasi lintas akun dan failback lintas akun.

`AWSElasticDisasterRecoveryCrossAccountReplicationPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryCrossAccountReplicationPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Mei 2023, 07:16 UTC
- Waktu teredit: 17 Januari 2024, 13:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryCrossAccountReplicationPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CrossAccountPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeInstances",
        "drs:DescribeSourceServers",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:CreateSourceServerForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CrossAccountPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticDisasterRecoveryEc2InstancePolicy

Deskripsi: Kebijakan ini memungkinkan menginstal dan menggunakan Agen AWS Replikasi, yang digunakan oleh AWS Elastic Disaster Recovery (DRS) untuk memulihkan server sumber yang berjalan di EC2 (lintas wilayah atau lintas AZ). Peran IAM dengan kebijakan ini harus dilampirkan (sebagai Profil Instans EC2) ke Instans EC2.

`AWSElasticDisasterRecoveryEc2InstancePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryEc2InstancePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Mei 2022, 12:30 UTC
- Waktu teredit: 27 November 2023, 13:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSEc2InstancePolicy1",
      "Effect" : "Allow",
      "Action" : [
```

```
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:CreateSourceServerForDrs",
        "drs:CreateSourceNetwork"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSEc2InstancePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    },
    {
      "Sid" : "DRSEc2InstancePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-network/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceNetwork"
        }
      }
    },
    {
      "Sid" : "DRSEc2InstancePolicy4",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
```

```
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSEc2InstancePolicy5",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/DRSCrossAccountAgentAuthorizedRole_*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SourceInstanceARN" : "${ec2:SourceInstanceARN}"
        },
        "ForAnyValue:StringEquals" : {
          "sts:TransitiveTagKeys" : "SourceInstanceARN"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticDisasterRecoveryFailbackInstallationPolicy

Deskripsi: Anda dapat melampirkan AWSElasticDisasterRecoveryFailbackInstallationPolicy kebijakan ke identitas IAM Anda. Kebijakan ini memungkinkan menginstal Elastic Disaster Recovery Failback

Client, yang digunakan untuk mengembalikan Instans Pemulihan kembali ke infrastruktur sumber asli Anda. Lampirkan kebijakan ini ke pengguna atau peran IAM yang kredensialnya Anda berikan saat menjalankan Klien Failback Pemulihan Bencana Elastic.

`AWSElasticDisasterRecoveryFailbackInstallationPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryFailbackInstallationPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 November 2021, 11:02 UTC
- Waktu teredit: 27 November 2023, 13:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryFailbackInstallationPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSFailbackInstallationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
```

```
        "drs:DescribeRecoveryInstances",
        "drs:DescribeSourceServers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackInstallationPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource",
        "drs:IssueAgentCertificateForDrs",
        "drs:AssociateFailbackClientToRecoveryInstanceForDrs",
        "drs:GetSuggestedFailbackClientDeviceMappingForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateFailbackClientDeviceMappingForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticDisasterRecoveryFailbackPolicy

Deskripsi: Kebijakan ini memungkinkan penggunaan Klien Failback Pemulihan Bencana Elastis, yang digunakan untuk mengembalikan Instans Pemulihan kembali ke infrastruktur sumber asli Anda. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSElasticDisasterRecoveryFailbackPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryFailbackPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 17 November 2021, 10:41 UTC
- Waktu teredit: 22 Juli 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSFailbackPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetChannelCommandsForDrs",
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "DRSFailbackPolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeReplicationServerAssociationsForDrs",
        "drs:DescribeRecoveryInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy4",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetFailbackCommandForDrs",
        "drs:UpdateFailbackClientLastSeenForDrs",
        "drs:NotifyAgentAuthenticationForDrs",
        "drs:UpdateAgentReplicationProcessStateForDrs",
        "drs:NotifyAgentReplicationProgressForDrs",
        "drs:NotifyAgentConnectedForDrs",
        "drs:NotifyAgentDisconnectedForDrs",
        "drs:NotifyConsistencyAttainedForDrs",
        "drs:GetFailbackLaunchRequestedForDrs",
        "drs:IssueAgentCertificateForDrs",
        "drs:GetAgentSnapshotCreditsForDrs",
        "drs:SendVolumeStatsForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/${aws:SourceIdentity}"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticDisasterRecoveryLaunchActionsPolicy

Deskripsi: Kebijakan ini memungkinkan Anda menggunakan Amazon SSM dan izin layanan tambahan yang diperlukan untuk menjalankan tindakan pasca-peluncuran di AWS Elastic Disaster Recovery (AWS DRS). Lampirkan kebijakan ini ke peran atau pengguna IAM Anda.

`AWSElasticDisasterRecoveryLaunchActionsPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryLaunchActionsPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 September 2023, 07:38 UTC
- Waktu teredit: 18 Juni 2026, 22:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryLaunchActionsPolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LaunchActionsPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
```

```
        "ssm:DescribeParameters"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-definition/*:*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
```

```
        "arn:aws:ssm:*::document/AWS-*",
        "arn:aws:ssm:*::document/AWSCodeDeployAgent-*",
        "arn:aws:ssm:*::document/AWSConfigRemediation-*",
        "arn:aws:ssm:*::document/AWSConformancePacks-*",
        "arn:aws:ssm:*::document/AWSDisasterRecovery-*",
        "arn:aws:ssm:*::document/AWSDistroOTel-*",
        "arn:aws:ssm:*::document/AWSDocs-*",
        "arn:aws:ssm:*::document/AWSDRS-*",
        "arn:aws:ssm:*::document/AWSEC2-*",
        "arn:aws:ssm:*::document/AWSEC2Launch-*",
        "arn:aws:ssm:*::document/AWSFIS-*",
        "arn:aws:ssm:*::document/AWSFleetManager-*",
        "arn:aws:ssm:*::document/AWSIncidents-*",
        "arn:aws:ssm:*::document/AWSKinesisTap-*",
        "arn:aws:ssm:*::document/AWSMigration-*",
        "arn:aws:ssm:*::document/AWSNVMe-*",
        "arn:aws:ssm:*::document/AWSNitroEnclavesWindows-*",
        "arn:aws:ssm:*::document/AWSObservabilityExporter-*",
        "arn:aws:ssm:*::document/AWSPVDriver-*",
        "arn:aws:ssm:*::document/AWSQuickSetupType-*",
        "arn:aws:ssm:*::document/AWSQuickStarts-*",
        "arn:aws:ssm:*::document/AWSRefactorSpaces-*",
        "arn:aws:ssm:*::document/AWSResilienceHub-*",
        "arn:aws:ssm:*::document/AWSSAP-*",
        "arn:aws:ssm:*::document/AWSSAPTools-*",
        "arn:aws:ssm:*::document/AWSSQLServer-*",
        "arn:aws:ssm:*::document/AWSSSO-*",
        "arn:aws:ssm:*::document/AWSSupport-*",
        "arn:aws:ssm:*::document/AWSSystemsManagerSAP-*",
        "arn:aws:ssm:*::document/AmazonCloudWatch-*",
        "arn:aws:ssm:*::document/AmazonCloudWatchAgent-*",
        "arn:aws:ssm:*::document/AmazonECS-*",
        "arn:aws:ssm:*::document/AmazonEFSUtils-*",
        "arn:aws:ssm:*::document/AmazonEKS-*",
        "arn:aws:ssm:*::document/AmazonInspector-*",
        "arn:aws:ssm:*::document/AmazonInspector2-*",
        "arn:aws:ssm:*::document/AmazonInternal-*",
        "arn:aws:ssm:*::document/AwsEnaNetworkDriver-*",
        "arn:aws:ssm:*::document/AwsVssComponents-*",
        "arn:aws:ssm:*::automation-definition/AWS-*:*",
        "arn:aws:ssm:*::automation-definition/AWSCodeDeployAgent-*:*",
        "arn:aws:ssm:*::automation-definition/AWSConfigRemediation-*:*",
        "arn:aws:ssm:*::automation-definition/AWSConformancePacks-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDisasterRecovery-*:*",
```

```
        "arn:aws:ssm:*::automation-definition/AWSDistroOTel-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDocs-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDRS-*:*",
        "arn:aws:ssm:*::automation-definition/AWSEC2-*:*",
        "arn:aws:ssm:*::automation-definition/AWSEC2Launch-*:*",
        "arn:aws:ssm:*::automation-definition/AWSFIS-*:*",
        "arn:aws:ssm:*::automation-definition/AWSFleetManager-*:*",
        "arn:aws:ssm:*::automation-definition/AWSIncidents-*:*",
        "arn:aws:ssm:*::automation-definition/AWSKinesisTap-*:*",
        "arn:aws:ssm:*::automation-definition/AWSMigration-*:*",
        "arn:aws:ssm:*::automation-definition/AWSNVMe-*:*",
        "arn:aws:ssm:*::automation-definition/AWSNitroEnclavesWindows-*:*",
        "arn:aws:ssm:*::automation-definition/AWSObservabilityExporter-*:*",
        "arn:aws:ssm:*::automation-definition/AWSPVDriver-*:*",
        "arn:aws:ssm:*::automation-definition/AWSQuickSetupType-*:*",
        "arn:aws:ssm:*::automation-definition/AWSQuickStarts-*:*",
        "arn:aws:ssm:*::automation-definition/AWSRefactorSpaces-*:*",
        "arn:aws:ssm:*::automation-definition/AWSResilienceHub-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSAP-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSAPTools-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSQLServer-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSSO-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSupport-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSystemsManagerSAP-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonCloudWatch-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonCloudWatchAgent-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonECS-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonEFSUtils-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonEKS-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInspector-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInspector2-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInternal-*:*",
        "arn:aws:ssm:*::automation-definition/AwsEnaNetworkDriver-*:*",
        "arn:aws:ssm:*::automation-definition/AwsVssComponents-*:*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "LaunchActionsPolicy4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy6",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:ListDocuments",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LaunchActionsPolicy7",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocumentVersions",
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "LaunchActionsPolicy8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy9",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy10",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy11",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "drs.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticDisasterRecoveryNetworkReplicationPolicy

Deskripsi: Kebijakan ini memungkinkan AWS Elastic Disaster Recovery (DRS) mendukung replikasi jaringan.

`AWSElasticDisasterRecoveryNetworkReplicationPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryNetworkReplicationPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 Juni 2023, 12:36 UTC
- Waktu teredit: 02 Januari 2024, 13:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryNetworkReplicationPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSNetworkReplicationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcAttribute",
```

```
        "ec2:DescribeInternetGateways",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeInstances",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetManagedPrefixListAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticDisasterRecoveryReadOnlyAccess

Deskripsi: Anda dapat melampirkan AWSElasticDisasterRecoveryReadOnlyAccess kebijakan ke identitas IAM Anda. Kebijakan ini memberikan izin ke semua API publik read-only dari Elastic Disaster Recovery (DRS), serta beberapa API read-only dari AWS layanan lain yang diperlukan untuk menggunakan konsol DRS secara penuh baca-saja. Lampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSElasticDisasterRecoveryReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 November 2021, 10:50 UTC
- Waktu teredit: 18 Agustus 2026, 14:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSReadOnlyAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeJobLogItems",
        "drs:DescribeJobs",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeRecoverySnapshots",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:DescribeSourceServers",
        "drs:GetFailbackReplicationConfiguration",
        "drs:GetLaunchConfiguration",
        "drs:GetReplicationConfiguration",
        "drs:ListExtensibleSourceServers",
        "drs:ListStagingAccounts",
        "drs:ListTagsForResource",
        "drs:ListLaunchActions"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "DRSReadOnlyAccess2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:GetInstanceTypesFromInstanceRequirements"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess4",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess5",
      "Effect" : "Allow",
      "Action" : "ssm:ListCommandInvocations",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess6",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameter",
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecovery-*"
    },
    {
      "Sid" : "DRSReadOnlyAccess7",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-CreateImage",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateNetworkConnectivity",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyMountedVolumes",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateHttpResponse",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateDiskSpace",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyProcessIsRunning",
```

```
        "arn:aws:ssm:*:*:document/AWSMigration-LinuxTimeSyncSetting",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure"
      ]
    },
    {
      "Sid" : "DRSReadOnlyAccess8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSReadOnlyAccess9",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetRecoveryPlan",
        "drs:ListRecoveryPlans",
        "drs:GetRecoveryPlanStep",
        "drs:ListRecoveryPlanSteps",
        "drs:GetRecoveryPlanExecution",
        "drs:ListRecoveryPlanExecutions",
        "drs:GetRecoveryPlanExecutionStep",
        "drs:ListRecoveryPlanExecutionSteps"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticDisasterRecoveryRecoveryInstancePolicy

Deskripsi: Kebijakan ini dilampirkan ke peran instans Instans Pemulihan Elastic Disaster Recovery. Kebijakan ini memungkinkan Instans Pemulihan Elastic Disaster Recovery (DRS), yang merupakan instans EC2 yang diluncurkan oleh Elastic Disaster Recovery - berkomunikasi dengan layanan DRS, dan dapat gagal kembali ke infrastruktur sumber aslinya. Peran IAM dengan kebijakan ini dilampirkan (sebagai Profil Instans EC2) oleh Elastic Disaster Recovery ke Instans Pemulihan DRS. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSElasticDisasterRecoveryRecoveryInstancePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryRecoveryInstancePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 17 November 2021, 10:20 UTC
- Waktu teredit: 27 November 2023, 13:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryRecoveryInstancePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "DRSRecoveryInstancePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs",
        "drs:UpdateReplicationCertificateForDrs",
        "drs:NotifyReplicationServerAuthenticationForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*",
      "Condition" : {
        "StringEquals" : {
          "drs:EC2InstanceARN" : "${ec2:SourceInstanceARN}"
        }
      }
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeRecoveryInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy4",
      "Effect" : "Allow",
      "Action" : [
```

```
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:CreateSourceServerForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy5",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy6",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy7",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/service-role/DRSCrossAccountAgentAuthorizedRole_*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SourceInstanceARN" : "${ec2:SourceInstanceARN}"
        },
        "ForAnyValue:StringEquals" : {
          "sts:TransitiveTagKeys" : "SourceInstanceARN"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticDisasterRecoveryReplicationServerPolicy

Deskripsi: Kebijakan ini dilampirkan ke peran instans server Elastic Disaster Recovery Replication. Kebijakan ini memungkinkan Server Replikasi Pemulihan Bencana Elastis (DRS), yang merupakan instans EC2 yang diluncurkan oleh Elastic Disaster Recovery - untuk berkomunikasi dengan layanan DRS, dan membuat snapshot EBS di layanan Anda. Akun AWS Peran IAM dengan kebijakan ini dilampirkan (sebagai Profil Instans EC2) oleh Elastic Disaster Recovery ke Server Replikasi DRS yang secara otomatis diluncurkan dan dihentikan oleh DRS, sesuai kebutuhan. Server Replikasi DRS digunakan untuk memfasilitasi replikasi data dari server eksternal Anda ke AWS, sebagai bagian dari proses pemulihan yang dikelola oleh DRS. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSElasticDisasterRecoveryReplicationServerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryReplicationServerPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 17 November 2021, 13:34 UTC
- Waktu teredit: 27 November 2023, 13:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSReplicationServerPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetChannelCommandsForDrs",
```

```
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentSnapshotCreditsForDrs",
        "drs:DescribeReplicationServerAssociationsForDrs",
        "drs:DescribeSnapshotRequestsForDrs",
        "drs:BatchDeleteSnapshotRequestForDrs",
        "drs:NotifyAgentAuthenticationForDrs",
        "drs:BatchCreateVolumeSnapshotGroupForDrs",
        "drs:UpdateAgentReplicationProcessStateForDrs",
        "drs:NotifyAgentReplicationProgressForDrs",
        "drs:NotifyAgentConnectedForDrs",
        "drs:NotifyAgentDisconnectedForDrs",
        "drs:NotifyVolumeEventForDrs",
        "drs:SendVolumeStatsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy4",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy5",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "DRSReplicationServerPolicy6",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSReplicationServerPolicy7",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticDisasterRecoveryServiceRolePolicy

Deskripsi: Kebijakan ini memungkinkan Elastic Disaster Recovery mengelola AWS sumber daya atas nama Anda.

`AWSElasticDisasterRecoveryServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 17 November 2021, 10:56 UTC
- Waktu teredit: 05 Januari 2025, 14:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticDisasterRecoveryServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSServiceRolePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy2",
      "Effect" : "Allow",
      "Action" : [
```

```
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:CreateRecoveryInstanceForDrs",
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy4",
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy5",
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy6",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeAttribute",
        "ec2:GetEbsDefaultKmsKeyId",
```

```
        "ec2:GetEbsEncryptionByDefault",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetManagedPrefixListAssociations",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeregisterImage"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
```

```
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy16",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
```

```
      "Sid" : "DRSServiceRolePolicy23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ]
    },
    {
      "Sid" : "DRSServiceRolePolicy25",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryReplicationServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "DRSServiceRolePolicy26",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy28",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "DRSServiceRolePolicy29",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy30",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy31",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "DRSServiceRolePolicy32",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
```

```
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy33",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticDisasterRecoveryStagingAccountPolicy

Deskripsi: Kebijakan ini mengizinkan akses baca-saja ke sumber daya AWS Elastic Disaster Recovery (DRS) seperti server sumber dan pekerjaan. Ini juga memungkinkan membuat snapshot yang dikonversi dan berbagi snapshot EBS itu dengan akun tertentu.

`AWSElasticDisasterRecoveryStagingAccountPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryStagingAccountPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Mei 2022, 09:49 UTC
- Waktu teredit: 27 November 2023, 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSStagingAccountPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers",
        "drs:DescribeRecoverySnapshots",
        "drs:CreateConvertedSnapshotForDrs",
        "drs:GetReplicationConfiguration",
        "drs:DescribeJobs",
        "drs:DescribeJobLogItems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSStagingAccountPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Add/userId" : "${aws:SourceIdentity}"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

Deskripsi: Kebijakan ini digunakan oleh AWS Elastic Disaster Recovery (DRS) untuk memulihkan server sumber ke akun target terpisah dan mengizinkan kegagalan kembali. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda.

`AWSElasticDisasterRecoveryStagingAccountPolicy_v2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryStagingAccountPolicy_v2` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 05 Januari 2023, 12:11 UTC
- Waktu teredit: 09 September 2026, 13:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSStagingAccountPolicyv21",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers",
        "drs:DescribeRecoverySnapshots",
        "drs:CreateConvertedSnapshotForDrs",
        "drs:GetReplicationConfiguration",
        "drs:DescribeJobs",
        "drs:DescribeJobLogItems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSStagingAccountPolicyv22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:Add/userId" : "${aws:SourceIdentity}"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSStagingAccountPolicyv23",
      "Effect" : "Allow",
      "Action" : "drs:IssueAgentCertificateForDrs",
      "Resource" : [
        "arn:aws:drs:*:*:source-server/*"
      ]
    },
    {
      "Sid" : "DRSStagingAccountPolicyv24",
      "Effect" : "Allow",
      "Action" : [
        "drs:CreateSourceServerForDrs",
        "drs:DescribeReplicationConfigurationTemplates"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticLoadBalancingClassicServiceRolePolicy

Deskripsi: Kebijakan Peran Terkait Layanan untuk Pesawat Kontrol Penyeimbangan Beban AWS Elastis - Klasik

`AWSElasticLoadBalancingClassicServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 19 September 2017, 22:36 UTC
- Waktu teredit: 07 Oktober 2019, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeVpcClassicLink",
        "ec2:CreateSecurityGroup",
```

```
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElasticLoadBalancingServiceRolePolicy

Deskripsi: Kebijakan Peran Terkait Layanan untuk Pesawat Kontrol Penyeimbangan Beban AWS Elastis

`AWSElasticLoadBalancingServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 19 September 2017, 22:19 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeVpcClassicLink",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:GetCoipPoolUsage",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
```

```
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssignIpv6Addresses",
        "ec2:ReleaseAddress",
        "ec2:UnassignIpv6Addresses",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeAvailabilityZones",
        "ec2:AllocateIpamPoolCidr",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "outposts:GetOutpostInstanceTypes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElementalMediaConnectCreateBridge

Deskripsi: Menyediakan akses penuh untuk membuat MediaConnect Gateway Bridges dan semua sub-sumber daya terkaitnya.

`AWSElementalMediaConnectCreateBridge`eadalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaConnectCreateBridge` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Maret 2026, 16:57 UTC

- Waktu teredit: 19 Maret 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectCreateBridge`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:CreateBridge",
        "mediaconnect:AddBridgeSources",
        "mediaconnect:AddBridgeOutputs"
      ],
      "Resource" : [
        "arn:aws:mediaconnect:*:*:bridge:*:*",
        "arn:aws:mediaconnect:*:*:bridge:*:*/bridgeSource/*",
        "arn:aws:mediaconnect:*:*:bridge:*:*/bridgeOutput/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElementalMediaConnectCreateFlow

Deskripsi: Menyediakan akses penuh untuk membuat MediaConnect Alur dan semua sub-sumber daya terkaitnya.

`AWSElementalMediaConnectCreateFlow`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaConnectCreateFlow` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Maret 2026, 16:57 UTC
- Waktu teredit: 19 Maret 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectCreateFlow`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : "mediaconnect.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:CreateFlow",
        "mediaconnect:AddFlowSources",
        "mediaconnect:AddFlowOutputs",
        "mediaconnect:GrantFlowEntitlements",
        "mediaconnect:AddFlowMediaStreams",
        "mediaconnect:AddFlowVpcInterfaces",
        "mediaconnect:TagResource"
      ],
      "Resource" : [
        "arn:aws:mediaconnect:*:*:flow:*:*",
        "arn:aws:mediaconnect:*:*:source:*:*",
        "arn:aws:mediaconnect:*:*:output:*:*",
        "arn:aws:mediaconnect:*:*:entitlement:*:*",
        "arn:aws:mediaconnect:*:*:flow:*:*/vpcInterface/*",
        "arn:aws:mediaconnect:*:*:flow:*:*/mediaStream/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElementalMediaConnectDeleteBridge

Deskripsi: Menyediakan akses penuh untuk menghapus MediaConnect Gateway Bridges dan semua sub-sumber daya terkaitnya.

`AWSElementalMediaConnectDeleteBridge`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaConnectDeleteBridge` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Maret 2026, 19:57 UTC
- Waktu teredit: 19 Maret 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectDeleteBridge`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DeleteBridge",
        "mediaconnect:RemoveBridgeSource",
        "mediaconnect:RemoveBridgeOutput"
      ],
      "Resource" : [
        "arn:aws:mediaconnect:*:*:bridge:*:*",
        "arn:aws:mediaconnect:*:*:bridge:*:*/bridgeSource/*",
        "arn:aws:mediaconnect:*:*:bridge:*:*/bridgeOutput/*"
      ]
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElementalMediaConnectDeleteFlow

Deskripsi: Menyediakan akses penuh untuk menghapus MediaConnect Alur dan semua sub-sumber daya terkaitnya.

`AWSElementalMediaConnectDeleteFlow`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaConnectDeleteFlow` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Maret 2026, 19:57 UTC
- Waktu teredit: 19 Maret 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectDeleteFlow`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DeleteFlow",
        "mediaconnect:RemoveFlowSource",
        "mediaconnect:RemoveFlowOutput",
        "mediaconnect:RevokeFlowEntitlement",
        "mediaconnect:RemoveFlowMediaStream",
        "mediaconnect:RemoveFlowVpcInterface"
      ],
      "Resource" : [
        "arn:aws:mediaconnect:*:*:flow:*:*",
        "arn:aws:mediaconnect:*:*:source:*:*",
        "arn:aws:mediaconnect:*:*:output:*:*",
        "arn:aws:mediaconnect:*:*:entitlement:*:*",
        "arn:aws:mediaconnect:*:*:flow:*:*/vpcInterface/*",
        "arn:aws:mediaconnect:*:*:flow:*:*/mediaStream/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElementalMediaConnectFullAccess

Deskripsi: Menyediakan akses penuh ke MediaConnect sumber daya AWS Elemental.

`AWSElementalMediaConnectFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaConnectFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Februari 2025, 20:07 UTC
- Waktu teredit: 12 Februari 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElementalMediaConnectReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke sumber daya AWS Elemental MediaConnect .

`AWSElementalMediaConnectReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaConnectReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Februari 2025, 20:07 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "mediaconnect:ListBridges",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGatewayInstances",
        "mediaconnect:ListGateways",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mediaconnect:DescribeBridge",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeFlowSourceMetadata",
        "mediaconnect:DescribeFlowSourceThumbnail",
        "mediaconnect:DescribeGateway",
        "mediaconnect:DescribeGatewayInstance",
        "mediaconnect:DescribeOffering",
        "mediaconnect:DescribeReservation",
        "mediaconnect:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElementalMediaConvertFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Elemental MediaConvert melalui Konsol Manajemen AWS dan SDK.

`AWSElementalMediaConvertFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaConvertFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Juni 2018, 19:25 UTC
- Waktu teredit: 10 Juni 2019, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "mediaconvert.amazonaws.com"
          ]
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElementalMediaConvertReadOnly

Deskripsi: Menyediakan akses baca saja ke AWS Elemental MediaConvert melalui Konsol Manajemen AWS dan SDK.

`AWSElementalMediaConvertReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaConvertReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Juni 2018, 19:25 UTC
- Waktu teredit: 10 Juni 2019, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "mediaconvert:DescribeEndpoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElementalMediaLiveFullAccess

Deskripsi: Menyediakan akses penuh ke sumber AWS daya Elemental MediaLive

`AWSElementalMediaLiveFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaLiveFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Juli 2020, 17:07 UTC
- Waktu teredit: 08 Juli 2020, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "medialive:*",
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElementalMediaLiveReadOnly

Deskripsi: Menyediakan akses baca saja ke sumber AWS daya Elemental MediaLive

`AWSElementalMediaLiveReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaLiveReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Juli 2020, 16:38 UTC
- Waktu teredit: 22 Juli 2024, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSElementalMediaLiveReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "medialive:Get*",
```

```
        "medialive:List*",
        "medialive:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElementalMediaPackageFullAccess

Deskripsi: Menyediakan akses penuh ke sumber AWS daya Elemental MediaPackage

`AWSElementalMediaPackageFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaPackageFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 Desember 2017, 23:39 UTC
- Waktu teredit: 29 Desember 2017, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackage:*",
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElementalMediaPackageReadOnly

Deskripsi: Menyediakan akses baca saja ke sumber AWS daya Elemental MediaPackage

`AWSElementalMediaPackageReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaPackageReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Desember 2017, 00:04 UTC

- Waktu teredit: 30 Desember 2017, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackage:List*",
      "mediapackage:Describe*"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElementalMediaPackageV2FullAccess

Deskripsi: Menyediakan akses penuh ke sumber daya AWS Elemental MediaPackage V2.

`AWSElementalMediaPackageV2FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaPackageV2FullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Juli 2023, 20:29 UTC
- Waktu teredit: 25 Juli 2023, 20:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElementalMediaPackageV2ReadOnly

Deskripsi: Menyediakan akses baca-saja ke sumber daya AWS Elemental V2 MediaPackage.

`AWSElementalMediaPackageV2ReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaPackageV2ReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Juli 2023, 20:31 UTC
- Waktu teredit: 25 Juli 2023, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackagev2:List*",
      "mediapackagev2:Get*"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElementalMediaStoreFullAccess

Deskripsi: Menyediakan akses baca dan tulis penuh ke semua MediaStore API

`AWSElementalMediaStoreFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaStoreFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Maret 2018, 23:15 UTC
- Waktu teredit: 05 Maret 2018, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElementalMediaStoreReadOnly

Deskripsi: Menyediakan izin baca-saja untuk API MediaStore

`AWSElementalMediaStoreReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaStoreReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Maret 2018, 19:48 UTC

- Waktu teredit: 08 Maret 2018, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:Get*",
        "mediastore:List*",
        "mediastore:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElementalMediaTailorFullAccess

Deskripsi: Menyediakan akses penuh ke sumber AWS daya Elemental MediaTailor

`AWSElementalMediaTailorFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaTailorFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 November 2021, 00:04 UTC
- Waktu teredit: 23 November 2021, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediatailor:*",
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSElementalMediaTailorReadOnly

Deskripsi: Menyediakan akses baca saja ke sumber AWS daya Elemental MediaTailor

`AWSElementalMediaTailorReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElementalMediaTailorReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 November 2021, 00:05 UTC
- Waktu teredit: 23 November 2021, 00:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediatailor:List*",
      "mediatailor:Describe*",
      "mediatailor:Get*"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSEnhancedClassicNetworkingMangementPolicy

Deskripsi: Kebijakan untuk mengaktifkan fitur manajemen jaringan klasik yang disempurnakan.

`AWSEnhancedClassicNetworkingMangementPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 20 September 2017, 17:29 UTC
- Waktu teredit: 20 September 2017, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSEntityResolutionConsoleFullAccess

Deskripsi: Menyediakan akses penuh konsol ke Res AWS olusi Entitas dan layanan terkait.

`AWSEntityResolutionConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSEntityResolutionConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Agustus 2023, 17:54 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EntityResolutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "entityresolution:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueSourcesConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetSchema",
        "glue:SearchTables",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
```

```
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3BucketsConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3SourcesConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListBucketVersions",
        "s3:GetBucketVersioning"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TaggingConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "ListRolesToPickRoleForPassing",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToEntityResolutionService",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*entityresolution*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "entityresolution.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageEventBridgeRules",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/entity-resolution-automatic*"
      ]
    },
    {
      "Sid" : "ADXReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:GetDataSet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CustomerProfilesIntegrationReadAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "connect:ListInstances",
        "profile:ListDomains",
        "profile:GetDomain",
        "profile:ListIntegrations",
        "profile:ListAccountIntegrations",
        "profile:ListProfileObjectTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CustomerProfilesIntegrationWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "profile:PutProfileObjectType"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/*/object-types/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSEntityResolutionConsoleReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke Resolusi AWS Entitas melalui. Konsol Manajemen AWS

`AWSEntityResolutionConsoleReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSEntityResolutionConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Agustus 2023, 18:18 UTC
- Waktu teredit: 17 Agustus 2023, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EntityResolutionRead",
      "Effect" : "Allow",
      "Action" : [
        "entityresolution:Get*",
        "entityresolution:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSFaultInjectionSimulatorEC2Access

Deskripsi: Kebijakan ini memberikan izin Layanan Simulator Injeksi Kesalahan di EC2 dan layanan lain yang diperlukan untuk melakukan tindakan FIS.

`AWSFaultInjectionSimulatorEC2Access`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFaultInjectionSimulatorEC2Access` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Oktober 2022, 20:39 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowEc2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:SendSpotInstanceInterruptions",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "AllowEc2InstancesWithEncryptedEbsVolumes",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "AllowSSMSendOnEc2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
```

```
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Sid" : "AllowSSMStopOnEc2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:ListCommands"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeSubnets",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSubnets",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSFaultInjectionSimulatorECSAccess

Deskripsi: Kebijakan ini memberikan izin Layanan Simulator Injeksi Kesalahan di ECS dan layanan lain yang diperlukan untuk melakukan tindakan FIS.

`AWSFaultInjectionSimulatorECSAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFaultInjectionSimulatorECSAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Oktober 2022, 20:37 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Clusters",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:ListContainerInstances"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "Tasks",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecs:DescribeTasks",
        "ecs:StopTask"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task/*/*"
      ]
    },
    {
      "Sid" : "ContainerInstances",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateContainerInstancesState"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:container-instance/*/*"
      ]
    },
    {
      "Sid" : "ListTasks",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSend",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Sid" : "SSMList",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeContainerInstances",
      "Effect" : "Allow",
      "Action" : "ecs:DescribeContainerInstances",
      "Resource" : "arn:aws:ecs:*:*:container-instance/*/*"
    },
    {
      "Sid" : "DescribeInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeSubnets",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSubnets",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSFaultInjectionSimulatorEKSAccess

Deskripsi: Kebijakan ini memberikan izin Layanan Simulator Injeksi Kesalahan di EKS dan layanan lain yang diperlukan untuk melakukan tindakan FIS.

`AWSFaultInjectionSimulatorEKSAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFaultInjectionSimulatorEKSAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Oktober 2022, 20:34 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
```

```
    {
      "Sid" : "DescribeSubnets",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSubnets",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeCluster",
      "Effect" : "Allow",
      "Action" : "eks:DescribeCluster",
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "DescribeNodeGroup",
      "Effect" : "Allow",
      "Action" : "eks:DescribeNodegroup",
      "Resource" : "arn:aws:eks:*:*:nodegroup/*"
    },
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSFaultInjectionSimulatorNetworkAccess

Deskripsi: Kebijakan ini memberikan izin Layanan Simulator Injeksi Kesalahan di jaringan EC2 dan layanan lain yang diperlukan untuk melakukan tindakan FIS.

`AWSFaultInjectionSimulatorNetworkAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFaultInjectionSimulatorNetworkAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Oktober 2022, 20:32 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateTagsOnNetworkAcl",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkAcl",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "CreateNetworkAcl",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkAcl",
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteNetworkAcl",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAclEntry",
        "ec2:DeleteNetworkAcl"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkAclOnVpc",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkAcl",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "VpcActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeRouteTables",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReplaceNetworkAclAssociation",
      "Effect" : "Allow",
      "Action" : "ec2:ReplaceNetworkAclAssociation",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-acl/*"
      ]
    },
    {
      "Sid" : "GetManagedPrefixListEntries",
      "Effect" : "Allow",
      "Action" : "ec2:GetManagedPrefixListEntries",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*"
    },
    {
      "Sid" : "CreateRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:CreateRouteTable",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateRouteTableOnVpc",
      "Effect" : "Allow",
      "Action" : "ec2:CreateRouteTable",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "CreateTagsOnRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
```

```
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateRouteTable",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnNetworkInterface",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnPrefixList",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateManagedPrefixList",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "CreateRoute",
      "Effect" : "Allow",
      "Action" : "ec2:CreateRoute",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterface",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterfaceOnSubnet",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "DeleteNetworkInterface",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "CreateManagedPrefixList",
      "Effect" : "Allow",
      "Action" : "ec2:CreateManagedPrefixList",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteManagedPrefixList",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteManagedPrefixList",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyManagedPrefixList",
      "Effect" : "Allow",
      "Action" : "ec2:ModifyManagedPrefixList",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "ReplaceRouteTableAssociation",
      "Effect" : "Allow",
      "Action" : "ec2:ReplaceRouteTableAssociation",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "AssociateRouteTable",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:AssociateRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "DisassociateRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:DisassociateRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DisassociateRouteTableOnSubnet",
      "Effect" : "Allow",
      "Action" : "ec2:DisassociateRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "ModifyVpcEndpointOnRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:ModifyVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyVpcEndpoint",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:ModifyVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ]
    },
    {
      "Sid" : "TransitGatewayRouteTableAssociation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:AssociateTransitGatewayRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSFaultInjectionSimulatorRDSAccess

Deskripsi: Kebijakan ini memberikan izin Layanan Simulator Injeksi Kesalahan di RDS dan layanan lain yang diperlukan untuk melakukan tindakan FIS.

`AWSFaultInjectionSimulatorRDSAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFaultInjectionSimulatorRDSAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Oktober 2022, 20:30 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFailover",
      "Effect" : "Allow",
      "Action" : [
        "rds:FailoverDBCluster"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "AllowReboot",
      "Effect" : "Allow",
      "Action" : [
        "rds:RebootDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*"
      ]
```

```
    },
    {
      "Sid" : "DescribeResources",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSFaultInjectionSimulatorSSMAccess

Deskripsi: Kebijakan ini memberikan izin Layanan Simulator Injeksi Kesalahan di SSM dan layanan lain yang diperlukan untuk melakukan tindakan FIS.

`AWSFaultInjectionSimulatorSSMAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFaultInjectionSimulatorSSMAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Oktober 2022, 15:33 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/*:*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSFinSpaceServiceRolePolicy

Deskripsi: Kebijakan untuk mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Amazon FinSpace

`AWSFinSpaceServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 12 Mei 2023, 16:42 UTC
- Waktu teredit: 01 Desember 2023, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSFinSpaceServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
```

```
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/FinSpace",
            "AWS/Usage"
          ]
        }
      },
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSFMAdminFullAccess

Deskripsi: Akses penuh untuk Administrator AWS FM

`AWSFMAdminFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFMAdminFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Mei 2018, 18:06 UTC
- Waktu teredit: 20 Oktober 2022, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fms:*",
        "waf:*",
        "waf-regional:*",
        "elasticloadbalancing:SetWebACL",
        "firehose:ListDeliveryStreams",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "shield:GetSubscriptionState",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:CheckCapacity",
        "wafv2:PutLoggingConfiguration",
        "wafv2:ListAvailableManagedRuleGroupVersions",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:ListRuleGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fms.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListDelegatedAdministrators",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "fms.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSFMAdminReadOnlyAccess

Deskripsi: Akses baca saja untuk Administrator AWS FM yang memungkinkan pemantauan operasi AWS FM

`AWSFMAdminReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFMAdminReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Mei 2018, 20:07 UTC
- Waktu teredit: 31 Oktober 2022, 22.42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fms:Get*",
        "fms:List*",
```

```
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "firehose:ListDeliveryStreams",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "shield:GetSubscriptionState",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:CheckCapacity",
        "wafv2:ListAvailableManagedRuleGroupVersions",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:ListRuleGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "organizations:ServicePrincipal" : [
            "fms.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSFMMemberReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke tindakan AWS WAF untuk akun anggota AWS Firewall Manager

`AWSFMMemberReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFMMemberReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Mei 2018, 21:05 UTC
- Waktu teredit: 09 Mei 2018, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSForWordPressPluginPolicy

Deskripsi: Kebijakan yang dikelola AWS untuk Plugin Wordpress

`AWSForWordPressPluginPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSForWordPressPluginPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Oktober 2019, 00:27 UTC
- Waktu teredit: 03 September 2026, 20:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Permissions1",
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech",
        "polly:DescribeVoices",
        "translate:TranslateText"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Permissions2",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:CreateBucket",
```

```
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::audio_for_wordpress*",
        "arn:aws:s3:::audio-for-wordpress*"
      ]
    },
    {
      "Sid" : "Permissions3",
      "Effect" : "Allow",
      "Action" : [
        "acm:AddTagsToCertificate",
        "acm:DescribeCertificate",
        "acm:RequestCertificate",
        "cloudformation:CreateStack",
        "cloudfront:ListDistributions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "us-east-1"
        }
      }
    },
    {
      "Sid" : "Permissions4",
      "Effect" : "Allow",
      "Action" : [
        "acm:DeleteCertificate",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:UpdateStack",
        "cloudfront:CreateDistribution",
        "cloudfront:CreateInvalidation",
        "cloudfront:DeleteDistribution",
        "cloudfront:GetDistribution",
        "cloudfront:GetInvalidation",
        "cloudfront:TagResource",
        "cloudfront:UpdateDistribution"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/createdBy" : "AWSForWordPressPlugin"
        }
      }
    },
    {
      "Sid" : "CloudFormationTagOnCreateStack",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "us-east-1",
          "cloudformation:CreateAction" : "CreateStack"
        }
      }
    },
    {
      "Sid" : "CloudFormationTagOnUpdateStack",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/createdBy" : "AWSForWordPressPlugin",
          "cloudformation:CreateAction" : "UpdateStack"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSGitSyncServiceRolePolicy

Deskripsi: Kebijakan yang memungkinkan Kon AWS eksi Kode untuk menyinkronkan konten dari repositori git Anda

`AWSGitSyncServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 16 November 2023, 17:05 UTC
- Waktu teredit: 26 April 2024, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
```

```
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSGlobalAcceleratorSLRPolicy

Deskripsi: Kebijakan pemberian izin ke AWS Global Accelerator untuk mengelola Antarmuka Jaringan Elastis EC2 dan Grup Keamanan.

`AWSGlobalAcceleratorSLRPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 05 April 2019, 19:39 UTC
- Waktu teredit: 29 Oktober 2024, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Action1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSServiceName" : "GlobalAccelerator"
        }
      }
```

```
    },
    {
      "Sid" : "EC2Action3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ElbAction1",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action4",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSGlueConsoleFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Glue melalui Konsol Manajemen AWS

`AWSGlueConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGlueConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Agustus 2017, 13:37 UTC
- Waktu teredit: 10 September 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BaseAppPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBSubnetGroups",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplateSummary",
        "dynamodb:ListTables",
        "kms:ListAliases",
        "kms:DescribeKey",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListDashboards",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:DescribeRecipe"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*",
        "arn:aws:s3:::aws-glue-*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-glue*/*"
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-glue*/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/aws-glue-*/*"
        },
        "StringEquals" : {
          "ec2:ResourceTag/aws:cloudformation:logical-id" : "ZeppelinInstance"
        }
      }
    },
    {
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSGlueServiceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSGlueConsoleSageMakerNotebookFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Glue melalui Konsol Manajemen AWS dan akses ke instance notebook sagemaker.

`AWSGlueConsoleSageMakerNotebookFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGlueConsoleSageMakerNotebookFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Oktober 2018, 17:52 UTC
- Waktu teredit: 10 September 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "iam:ListRoles",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:CreateNetworkInterface",
        "ec2:AttachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "rds:DescribeDBInstances",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplateSummary",
        "dynamodb:ListTables",
        "kms:ListAliases",
        "kms:DescribeKey",
        "sagemaker:ListNotebookInstances",
```

```
        "cloudformation:ListStacks",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListDashboards"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/*aws-glue-*/*",
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-glue*/*"
```

```
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-glue*/*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StopNotebookInstance",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:ListTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance/aws-glue-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:ListNotebookInstanceLifecycleConfigs"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/aws-glue-
*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/aws-glue-*/*"
        },
        "StringEquals" : {
          "ec2:ResourceTag/aws:cloudformation:logical-id" : "ZeppelinInstance"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
```

```
            "aws-glue-*"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceSageMakerNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSGlueServiceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AwsGlueDataBrewFullAccessPolicy

Deskripsi: Menyediakan akses penuh ke AWS Glue DataBrew melalui Konsol Manajemen AWS. Juga menyediakan akses tertentu ke layanan terkait (misalnya, S3, KMS, Glue).

`AwsGlueDataBrewFullAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AwsGlueDataBrewFullAccessPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 November 2020, 16:51 UTC
- Waktu teredit: 04 Februari 2022 18.28 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "databrew:CreateDataset",
        "databrew:DescribeDataset",
        "databrew:ListDatasets",
        "databrew:UpdateDataset",
        "databrew:DeleteDataset",
        "databrew:CreateProject",
        "databrew:DescribeProject",
        "databrew:ListProjects",
        "databrew:StartProjectSession",
        "databrew:SendProjectSessionAction",
        "databrew:UpdateProject",
        "databrew:DeleteProject",
        "databrew:CreateRecipe",
        "databrew:DescribeRecipe",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:PublishRecipe",
```

```
        "databrew:UpdateRecipe",
        "databrew:BatchDeleteRecipeVersion",
        "databrew:DeleteRecipeVersion",
        "databrew:CreateRecipeJob",
        "databrew:CreateProfileJob",
        "databrew:DescribeJob",
        "databrew:DescribeJobRun",
        "databrew:ListJobRuns",
        "databrew:ListJobs",
        "databrew:StartJobRun",
        "databrew:StopJobRun",
        "databrew:UpdateProfileJob",
        "databrew:UpdateRecipeJob",
        "databrew:DeleteJob",
        "databrew:CreateSchedule",
        "databrew:DescribeSchedule",
        "databrew:ListSchedules",
        "databrew:UpdateSchedule",
        "databrew:DeleteSchedule",
        "databrew:CreateRuleset",
        "databrew:DeleteRuleset",
        "databrew:DescribeRuleset",
        "databrew:ListRulesets",
        "databrew:UpdateRuleset",
        "databrew:ListTagsForResource",
        "databrew:TagResource",
        "databrew:UntagResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:ListFlows",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables",
```

```
        "glue:GetDataCatalogEncryptionSettings",
        "dataexchange:ListDataSets",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:ListRevisionAssets",
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:GetJob",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "secretsmanager:ListSecrets",
        "secretsmanager:DescribeSecret",
        "sts:GetCallerIdentity",
        "cloudtrail:LookupEvents",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/AwsGlueDataBrew-*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*/awsgluedatabrew*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::databrew-public-datasets-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AwsGlueDataBrew-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateRandom"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "databrew.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "databrew!default"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "databrew.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "databrew.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSGlueDataBrewServiceRole

Deskripsi: Kebijakan ini memberikan izin perekat untuk melakukan tindakan pada katalog data lem pengguna, kebijakan ini juga memberikan izin untuk tindakan ec2 untuk mengizinkan lem membuat ENI untuk terhubung ke sumber daya di VPC, juga mengizinkan glue mengakses data terdaftar di lakeformation dan izin untuk mengakses cloudwatch pengguna

`AWSGlueDataBrewServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGlueDataBrewServiceRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 04 Desember 2020, 21:26 UTC
- Waktu teredit: 20 Maret 2024, 23:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetConnection"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "GluePIIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchGetCustomEntityTypes",
        "glue:GetCustomEntityType"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3PublicDatasetAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::databrew-public-datasets-*"
      ]
    },
    {
      "Sid" : "EC2NetworkingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2DeleteGlueNetworkInterfacePermissions",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws-glue-service-resource" : "*"
        }
      },
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "EC2GlueTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "GlueDatabrewLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws-glue-databrew/*"
      ]
    },
    {
      "Sid" : "LakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSGlueSchemaRegistryFullAccess

Deskripsi: Menyediakan akses penuh ke Layanan Registri Skema AWS Glue

`AWSGlueSchemaRegistryFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGlueSchemaRegistryFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 November 2020, 00:19 UTC
- Waktu teredit: 20 November 2020, 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGlueSchemaRegistryFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateRegistry",
        "glue:UpdateRegistry",
        "glue:DeleteRegistry",
        "glue:GetRegistry",
        "glue:ListRegistries",
        "glue:CreateSchema",
        "glue:UpdateSchema",
        "glue:DeleteSchema",
        "glue:GetSchema",
        "glue:ListSchemas",
        "glue:RegisterSchemaVersion",
        "glue:DeleteSchemaVersions",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:ListSchemaVersions",
        "glue:CheckSchemaVersionValidity",
        "glue:PutSchemaVersionMetadata",
        "glue:RemoveSchemaVersionMetadata",
        "glue:QuerySchemaVersionMetadata"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSGlueSchemaRegistryTagsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTags",
```

```
        "glue:TagResource",
        "glue:UnTagResource"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:schema/*",
        "arn:aws:glue:*:*:registry/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSGlueSchemaRegistryReadonlyAccess

Deskripsi: Menyediakan akses readonly ke Layanan Registri Skema AWS Glue

`AWSGlueSchemaRegistryReadonlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGlueSchemaRegistryReadonlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 November 2020, 00:20 UTC
- Waktu teredit: 20 November 2020, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadonlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGlueSchemaRegistryReadonlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetRegistry",
        "glue:ListRegistries",
        "glue:GetSchema",
        "glue:ListSchemas",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:ListSchemaVersions",
        "glue:GetSchemaVersionsDiff",
        "glue:CheckSchemaVersionValidity",
        "glue:QuerySchemaVersionMetadata",
        "glue:GetTags"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSGlueServiceNotebookRole

Deskripsi: Kebijakan untuk peran layanan AWS Glue yang memungkinkan pelanggan mengelola server notebook

`AWSGlueServiceNotebookRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGlueServiceNotebookRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Agustus 2017, 13:37 UTC
- Waktu teredit: 09 Oktober 2023, 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
```

```
        "glue:DeleteDatabase",
        "glue:DeletePartition",
        "glue:DeleteTable",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:UpdateDatabase",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:CreateConnection",
        "glue:CreateJob",
        "glue:DeleteConnection",
        "glue:DeleteJob",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:UpdateJob",
        "glue:BatchDeleteConnection",
        "glue:UpdateConnection",
        "glue:GetUserDefinedFunction",
        "glue:UpdateUserDefinedFunction",
        "glue:GetUserDefinedFunctions",
        "glue:DeleteUserDefinedFunction",
        "glue:CreateUserDefinedFunction",
        "glue:BatchGetPartition",
        "glue:BatchDeletePartition",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteTable",
        "glue:UpdateDevEndpoint",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*",
        "arn:aws:s3:::aws-glue*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSGlueServiceRole

Deskripsi: Kebijakan untuk peran layanan AWS Glue yang memungkinkan akses ke layanan terkait termasuk EC2, S3, dan Cloudwatch Logs

`AWSGlueServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGlueServiceRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Agustus 2017, 13:37 UTC
- Waktu teredit: 11 September 2023, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
```

```
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*",
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AwsGlueSessionUserRestrictedNotebookPolicy

Deskripsi: Menyediakan izin yang memungkinkan pengguna membuat dan menggunakan hanya sesi buku catatan yang terkait dengan pengguna. Kebijakan ini juga menyertakan izin untuk secara eksplisit mengizinkan pengguna untuk meneruskan peran sesi Glue yang dibatasi.

`AwsGlueSessionUserRestrictedNotebookPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AwsGlueSessionUserRestrictedNotebookPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 April 2022, 15:24 UTC
- Waktu teredit: 15 Agustus 2024, 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NotebokAllowActions0",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}",
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Sid" : "NotebookAllowActions1",
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "NotebookAllowActions2",
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Sid" : "NotebookAllowActions3",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "NotebookDenyActions",
      "Effect" : "Deny",
      "Action" : [
        "glue:UntagResource",
        "tag:TagResources",
```

```
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "NotebookPassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AwsGlueSessionServiceRoleUserRestrictedForNotebook*",
        "arn:aws:iam::*:role/AwsGlueSessionUserRestrictedNotebookServiceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AwsGlueSessionUserRestrictedNotebookServiceRole

Deskripsi: Menyediakan akses penuh ke semua sumber daya AWS Glue kecuali untuk sesi. Memungkinkan pengguna untuk membuat dan menggunakan hanya sesi buku catatan yang terkait dengan pengguna. Kebijakan ini juga mencakup izin lain yang diperlukan oleh AWS Glue untuk mengelola sumber daya Glue di AWS layanan lain.

`AwsGlueSessionUserRestrictedNotebookServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AwsGlueSessionUserRestrictedNotebookServiceRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 18 April 2022, 15:27 UTC
- Waktu teredit: 15 Agustus 2024, 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
```

```
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}",
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
```

```
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AwsGlueSessionUserRestrictedPolicy

Deskripsi: Menyediakan izin yang memungkinkan pengguna membuat dan menggunakan hanya sesi interaktif yang terkait dengan pengguna. Kebijakan ini juga menyertakan izin untuk secara eksplisit mengizinkan pengguna untuk meneruskan peran sesi Glue yang dibatasi.

`AwsGlueSessionUserRestrictedPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AwsGlueSessionUserRestrictedPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 April 2022, 21:31 UTC
- Waktu teredit: 05 Agustus 2024, 23:06 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSessionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:userid}"
        },
```

```
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}",
          "aws:RequestTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowCompletionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
```

```
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowListSessions",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DenyTagActions",
      "Effect" : "Deny",
      "Action" : [
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AwsGlueSessionServiceRoleUserRestricted*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AwsGlueSessionUserRestrictedServiceRole

Deskripsi: Menyediakan akses penuh ke semua sumber daya AWS Glue kecuali untuk sesi. Memungkinkan pengguna untuk membuat dan menggunakan hanya sesi interaktif yang terkait dengan pengguna. Kebijakan ini juga mencakup izin lain yang diperlukan oleh AWS Glue untuk mengelola sumber daya Glue di AWS layanan lain

`AwsGlueSessionUserRestrictedServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AwsGlueSessionUserRestrictedServiceRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 April 2022, 21:30 UTC

- Waktu teredit: 05 Agustus 2024, 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema/*"
      ]
    },
    {
      "Sid" : "AllowCompletionActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "AllowSessionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:userid}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}",
          "aws:RequestTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowStatementActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowListSessionsAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DenyTagActions",
      "Effect" : "Deny",
      "Action" : [
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Sid" : "AllowS3ObjectCrawlerActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*"
      ]
    },
    {
      "Sid" : "AllowLogsActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
```

```
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Sid" : "AllowTagsActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSGrafanaAccountAdministrator

Deskripsi: Menyediakan akses dalam Amazon Grafana untuk membuat dan mengelola ruang kerja untuk seluruh organisasi.

`AWSGrafanaAccountAdministrator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGrafanaAccountAdministrator` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Februari 2021, 00:20 UTC
- Waktu teredit: 15 Februari 2022, 22.36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaOrganizationAdmin",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrafanaIAMGetRolePermission",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/*"
```

```
    },
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrafanaIAMPassRolePermission",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "grafana.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSGrafanaConsoleReadOnlyAccess

Deskripsi: Akses ke operasi baca saja di Amazon Grafana.

`AWSGrafanaConsoleReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGrafanaConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Februari 2021, 00:10 UTC
- Waktu teredit: 15 Februari 2022, 22.30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaConsoleReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:Describe*",
        "grafana:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSGrafanaWorkspacePermissionManagement

Deskripsi: Hanya menyediakan kemampuan untuk memperbarui izin pengguna dan grup untuk ruang kerja AWS Grafana.

`AWSGrafanaWorkspacePermissionManagement`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGrafanaWorkspacePermissionManagement` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Februari 2021, 00:15 UTC
- Waktu teredit: 15 Maret 2023, 22:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
```

```
        "grafana:UpdatePermissions",
        "grafana:ListPermissions",
        "grafana:ListWorkspaces"
      ],
      "Resource" : "arn:aws:grafana:*:*:/workspaces*"
    },
    {
      "Sid" : "IAMIdentityCenterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:ListDirectoryAssociations",
        "sso:GetManagedApplicationInstance",
        "sso:ListProfiles",
        "sso:AssociateProfile",
        "sso:DisassociateProfile",
        "sso:GetProfile",
        "sso:ListProfileAssociations",
        "sso-directory:DescribeUser",
        "sso-directory:DescribeGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSGrafanaWorkspacePermissionManagementV2

Deskripsi: Menyediakan kemampuan untuk memperbarui izin pengguna dan grup IAM Identity Center (iDC) untuk ruang kerja Grafana yang Dikelola Amazon.

`AWSGrafanaWorkspacePermissionManagementV2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGrafanaWorkspacePermissionManagementV2` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Januari 2024, 18:39 UTC
- Waktu teredit: 05 Januari 2024, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:UpdatePermissions",
        "grafana:ListPermissions",
        "grafana:ListWorkspaces"
      ],
      "Resource" : "arn:aws:grafana:*:*:/workspaces*"
    },
    {
      "Sid" : "IAMIdentityCenterPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:ListDirectoryAssociations",
        "sso:GetManagedApplicationInstance",
        "sso:ListProfiles",
        "sso:GetProfile",
        "sso:ListProfileAssociations",
        "sso-directory:DescribeUser",
        "sso-directory:DescribeGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSGreengrassFullAccess

Deskripsi: Kebijakan ini memberikan akses penuh ke tindakan konfigurasi, manajemen, dan penerapan AWS Greengrass

`AWSGreengrassFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGreengrassFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Mei 2017, 00:47 UTC
- Waktu teredit: 03 Mei 2017, 00:47 UTC

- ARN: `arn:aws:iam::aws:policy/AWSGreengrassFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "greengrass:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSGreengrassReadOnlyAccess

Deskripsi: Kebijakan ini memberikan akses baca saja ke konfigurasi AWS Greengrass, manajemen, dan tindakan penerapan

`AWSGreengrassReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGreengrassReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Oktober 2018, 16:01 UTC
- Waktu teredit: 30 Oktober 2018, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "greengrass:List*",
        "greengrass:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSGreengrassResourceAccessRolePolicy

Deskripsi: Kebijakan untuk peran layanan AWS Greengrass yang memungkinkan akses ke layanan terkait termasuk bayangan hal AWS Lambda dan AWS IoT.

`AWSGreengrassResourceAccessRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGreengrassResourceAccessRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Februari 2017, 21:17 UTC
- Waktu teredit: 14 November 2018, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowGreengrassAccessToShadows",
```

```
      "Action" : [
        "iot:DeleteThingShadow",
        "iot:GetThingShadow",
        "iot:UpdateThingShadow"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iot:*:*:thing/GG_*",
        "arn:aws:iot:*:*:thing/*-gcm",
        "arn:aws:iot:*:*:thing/*-gda",
        "arn:aws:iot:*:*:thing/*-gci"
      ]
    },
    {
      "Sid" : "AllowGreengrassToDescribeThings",
      "Action" : [
        "iot:DescribeThing"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iot:*:*:thing/*"
    },
    {
      "Sid" : "AllowGreengrassToDescribeCertificates",
      "Action" : [
        "iot:DescribeCertificate"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iot:*:*:cert/*"
    },
    {
      "Sid" : "AllowGreengrassToCallGreengrassServices",
      "Action" : [
        "greengrass:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGreengrassToGetLambdaFunctions",
      "Action" : [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGreengrassToGetGreengrassSecrets",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:greengrass-*"
    },
    {
      "Sid" : "AllowGreengrassAccessToS3Objects",
      "Action" : [
        "s3:GetObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::*Greengrass*",
        "arn:aws:s3:::*GreenGrass*",
        "arn:aws:s3:::*greengrass*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowGreengrassAccessToS3BucketLocation",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGreengrassAccessToSageMakerTrainingJobs",
      "Action" : [
        "sagemaker:DescribeTrainingJob"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
      ]
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSGroundStationAgentInstancePolicy

Deskripsi: Menyediakan izin Instans Endpoint Aliran Dataflow untuk menggunakan Agen Stasiun G AWS round

`AWSGroundStationAgentInstancePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGroundStationAgentInstancePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 Maret 2023, 15:23 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "groundstation:RegisterAgent",
        "groundstation:UpdateAgentStatus",
        "groundstation:GetAgentConfiguration",
        "groundstation:GetAgentTaskResponseUrl"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWS Health_EventProcessorServiceRolePolicy

Deskripsi: AWS Mengizinkan Kesehatan mengaktifkan fitur prosesor acara Kesehatan.

`AWSHealth_EventProcessorServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran

- Waktu pembuatan: 13 Januari 2023, 19:24 UTC
- Waktu teredit: 13 Januari 2023, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealth_EventProcessorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "event-processor.health.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSHealthFullAccess

Deskripsi: Memungkinkan akses penuh ke Apis AWS Kesehatan dan Pemberitahuan dan Dasbor Kesehatan Pribadi

`AWSHealthFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSHealthFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Desember 2016, 12:30 UTC
- Waktu teredit: 16 November 2020, 18.11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "health.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "health:*",
        "organizations:ListAccounts",
        "organizations:ListParents",
        "organizations:DescribeAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "health.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSHealthImagingFullAccess

Deskripsi: Menyediakan akses penuh ke layanan AWS Health Imaging.

`AWSHealthImagingFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSHealthImagingFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Juli 2023, 23:39 UTC
- Waktu teredit: 25 Juli 2023, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "medical-imaging:*"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "medical-imaging.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSHealthImagingReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke layanan AWS Health Imaging.

`AWSHealthImagingReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSHealthImagingReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Juli 2023, 23:40 UTC
- Waktu teredit: 01 Agustus 2023, 15:18 UTC

- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "medical-imaging:GetDICOMImportJob",
        "medical-imaging:GetDatastore",
        "medical-imaging:GetImageFrame",
        "medical-imaging:GetImageSet",
        "medical-imaging:GetImageSetMetadata",
        "medical-imaging:ListDICOMImportJobs",
        "medical-imaging:ListDatastores",
        "medical-imaging:ListImageSetVersions",
        "medical-imaging:ListTagsForResource",
        "medical-imaging:SearchImageSets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSHealthImagingServiceRolePolicy

Deskripsi: Memberikan izin AWS HealthImaging untuk mengelola operasi layanan dan menerbitkan metrik layanan

`AWSHealthImagingServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 30 Januari 2026, 18:34 UTC
- Waktu teredit: 30 Januari 2026, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealthImagingServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/HealthImaging"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSHealthOmicsServiceLinkedRolePolicy

Deskripsi: Kebijakan Terkelola Untuk Peran HealthOmics Terkait Layanan Amazon

`AWSHealthOmicsServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 04 Maret 2026, 22:57 UTC
- Waktu teredit: 04 Maret 2026, 22:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealthOmicsServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowEC2DescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowVpcGetActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "AllowCreateNetworkInterfaceWithTag",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Service" : "HealthOmics"
        }
      }
    },
    {
```

```
      "Sid" : "AllowCreateNetworkInterfaceSubnetSecurityGroup",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "AllowCreateTags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "AllowDeleteNetworkInterface",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Service" : "HealthOmics"
        }
      }
    },
    {
      "Sid" : "AllowAssignUnassignPrivateIpAddresses",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Service" : "HealthOmics"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIAMIdentityCenterAllowListForIdentityContext

Deskripsi: Menyediakan daftar tindakan yang diizinkan untuk peran yang diasumsikan dengan konteks identitas Pusat Identitas IAM. AWS Layanan Token Keamanan (AWS STS) secara otomatis melampirkan kebijakan ini ke peran yang diasumsikan. Konteks identitas diteruskan sebagai ProvidedContext.

`AWSIAMIdentityCenterAllowListForIdentityContext`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIAMIdentityCenterAllowListForIdentityContext` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 November 2023, 15:21 UTC
- Waktu teredit: 01 Oktober 2024, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIAMIdentityCenterAllowListForIdentityContext`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedIdentityPropagation",
      "Effect" : "Deny",
      "NotAction" : [
        "aoss:APIAccessAll",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreatePreparedStatement",
        "athena:DeleteNamedQuery",
        "athena:DeletePreparedStatement",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetWorkGroup",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "athena:UpdateNamedQuery",
        "athena:UpdatePreparedStatement",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListTableMetadata",
        "athena:ListWorkGroups",
        "elasticmapreduce:GetClusterSessionCredentials",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:CancelSteps",
        "elasticmapreduce:DescribeStep",
```

```
        "elasticmapreduce:ListSteps",
        "es:ESHttpHead",
        "es:ESHttpPost",
        "es:ESHttpGet",
        "es:ESHttpPatch",
        "es:ESHttpDelete",
        "es:ESHttpPut",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersions",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:SearchTables",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchUpdatePartition",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "lakeformation:GetDataAccess",
        "s3:GetAccessGrantsInstanceForPrefix",
        "s3:GetDataAccess",
        "s3:ListCallerAccessGrants",
        "q:StartConversation",
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:StartTroubleshootingAnalysis",
```

```
        "q:GetTroubleshootingResults",
        "q:StartTroubleshootingResolutionExplanation",
        "q:UpdateTroubleshootingCommandResult",
        "qapps:CreateQApp",
        "qapps:PredictProblemStatementFromConversation",
        "qapps:PredictQAppFromProblemStatement",
        "qapps:CopyQApp",
        "qapps:GetQApp",
        "qapps:ListQApps",
        "qapps:UpdateQApp",
        "qapps:DeleteQApp",
        "qapps:AssociateQAppWithUser",
        "qapps:DisassociateQAppFromUser",
        "qapps:ImportDocumentToQApp",
        "qapps:ImportDocumentToQAppSession",
        "qapps:CreateLibraryItem",
        "qapps:GetLibraryItem",
        "qapps:UpdateLibraryItem",
        "qapps:CreateLibraryItemReview",
        "qapps:ListLibraryItems",
        "qapps:CreateSubscriptionToken",
        "qapps:StartQAppSession",
        "qapps:StopQAppSession",
        "qapps:PredictQApp",
        "qapps:ImportDocument",
        "qapps:AssociateLibraryItemReview",
        "qapps:DisassociateLibraryItemReview",
        "qapps:GetQAppSession",
        "qapps:UpdateQAppSession",
        "qapps:GetQAppSessionMetadata",
        "qapps:UpdateQAppSessionMetadata",
        "qapps:TagResource",
        "qapps:ListQAppSessionData",
        "qapps:ExportQAppSessionData",
        "qbusiness:Chat",
        "qbusiness:ChatSync",
        "qbusiness:ListConversations",
        "qbusiness:ListMessages",
        "qbusiness:DeleteConversation",
        "qbusiness:PutFeedback",
        "sts:SetContext"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIAMRoleManagerServiceRolePolicy

Deskripsi: Mengizinkan Manajer Peran IAM mengelola sumber daya di akun Anda atas nama Anda.

`AWSIAMRoleManagerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 15 Juli 2026, 23:57 UTC
- Waktu teredit: 05 Agustus 2026, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIAMRoleManagerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageServiceLinkedAnalyzer",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CreateServiceLinkedAnalyzer",
        "access-analyzer:DeleteServiceLinkedAnalyzer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateAccessAnalyzerServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "access-analyzer.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIdentityCenterExternalManagementPolicy

Deskripsi: Menyediakan akses untuk mengelola pengguna Pusat Identitas IAM dari penyedia eksternal.

`AWSIdentityCenterExternalManagementPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIdentityCenterExternalManagementPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 November 2025, 00:34 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIdentityCenterExternalManagementPolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IdentityStoreUserCreation",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:CreateUser"
      ],
      "Resource" : [
        "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/IdentityStoreId}",
        "arn:aws:identitystore:::user/*"
      ],
      "Condition" : {
        "ForAllValues:ArnEquals" : {
          "identitystore:UserExternalIdIssuers" : [
```

```
            "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/
IdentityStoreId}/provisioningtenant/${aws:PrincipalTag/IdentityStoreExternalIdIssuer}"
          ]
        },
        "Null" : {
          "identitystore:UserExternalIdIssuers" : "false",
          "identitystore:ReservedUserId" : "false"
        }
      }
    },
    {
      "Sid" : "IdentityStoreUserManagement",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:UpdateUser",
        "identitystore:DeleteUser",
        "identitystore:DescribeUser"
      ],
      "Resource" : [
        "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/IdentityStoreId}",
        "arn:aws:identitystore:::user/*"
      ],
      "Condition" : {
        "ForAllValues:ArnEquals" : {
          "identitystore:UserExternalIdIssuers" : [
            "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/
IdentityStoreId}/provisioningtenant/${aws:PrincipalTag/IdentityStoreExternalIdIssuer}"
          ]
        },
        "Null" : {
          "identitystore:UserExternalIdIssuers" : "false"
        }
      }
    },
    {
      "Sid" : "IdentityStoreCMKAccess",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : [
            "arn:aws:identitystore::${aws:PrincipalAccount}:identitystore/
${aws:PrincipalTag/IdentityStoreId}"
```

```
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIdentitySyncFullAccess

Deskripsi: Memberikan akses penuh ke layanan Identity Sync

`AWSIdentitySyncFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIdentitySyncFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Maret 2022, 23:29 UTC
- Waktu teredit: 23 Maret 2022, 23.29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication"
      ],
      "Resource" : "arn:*:ds:*:*:*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:DeleteSyncProfile",
        "identity-sync:CreateSyncProfile",
        "identity-sync:GetSyncProfile",
        "identity-sync:StartSync",
        "identity-sync:StopSync",
        "identity-sync:CreateSyncFilter",
        "identity-sync:DeleteSyncFilter",
        "identity-sync:ListSyncFilters",
        "identity-sync:CreateSyncTarget",
        "identity-sync:DeleteSyncTarget",
        "identity-sync:GetSyncTarget",
        "identity-sync:UpdateSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIdentitySyncReadOnlyAccess

Deskripsi: Akses baca saja ke layanan Identity Sync

`AWSIdentitySyncReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIdentitySyncReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Maret 2022, 23:29 UTC
- Waktu teredit: 23 Maret 2022, 23.29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "identity-sync:GetSyncProfile",
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSImageBuilderFullAccess

Deskripsi: Menyediakan akses penuh ke semua tindakan Pembuat AWS Gambar dan akses cakupan sumber daya ke AWS layanan terkait.

`AWSImageBuilderFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSImageBuilderFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 Desember 2019, 18:25 UTC
- Waktu teredit: 13 April 2021, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:*imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "license-manager:ListLicenseConfigurations",
        "license-manager:ListLicenseSpecificationsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/
AWSServiceRoleForImageBuilder"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/*imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:instance-profile/*imagebuilder*",
        "arn:aws:iam::*:role/*imagebuilder*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
```

```
      "Resource" : "arn:aws:s3::*:*imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/
AWSServiceRoleForImageBuilder",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "imagebuilder.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeVolumes",
        "ec2:DescribeSubnets",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplates"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSImageBuilderReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke semua tindakan Pembuat AWS Gambar.

`AWSImageBuilderReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSImageBuilderReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Desember 2019, 22:29 UTC
- Waktu teredit: 19 Desember 2019, 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:Get*",
        "imagebuilder:List*"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/
AWSServiceRoleForImageBuilder"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSImportExportFullAccess

Deskripsi: Menyediakan akses baca dan tulis ke pekerjaan yang dibuat di bawah Akun AWS.

`AWSImportExportFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSImportExportFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "importexport:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSImportExportReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke pekerjaan yang dibuat di bawah Akun AWS.

`AWSImportExportReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSImportExportReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "importexport:ListJobs",
        "importexport:GetStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIncidentManagerIncidentAccessServiceRolePolicy

Deskripsi: Memberikan izin Manajer Insiden untuk memang AWS gil layanan lain sebagai bagian dari pengelolaan insiden.

`AWSIncidentManagerIncidentAccessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIncidentManagerIncidentAccessServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 November 2023, 00:01 UTC
- Waktu teredit: 20 Februari 2024, 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerIncidentAccessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IncidentAccessPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIncidentManagerResolverAccess

Deskripsi: Kebijakan ini memberikan izin untuk memulai, melihat, dan memperbarui insiden dengan akses penuh ke peristiwa timeline kustom & item terkait. Tetapkan kebijakan ini kepada pengguna yang akan membuat dan menyelesaikan insiden.

`AWSIncidentManagerResolverAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIncidentManagerResolverAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 Mei 2021, 06:12 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC

- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:StartIncident",
        "ssm-contacts:StartEngagement"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResponsePlanReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:GetResponsePlan"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IncidentRecordResolverPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:GetIncidentRecord",
        "ssm-incidents:UpdateIncidentRecord",
        "ssm-incidents:ListTimelineEvents",
        "ssm-incidents:CreateTimelineEvent",
```

```
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:UpdateTimelineEvent",
        "ssm-incidents:DeleteTimelineEvent",
        "ssm-incidents:ListRelatedItems",
        "ssm-incidents:UpdateRelatedItems"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIncidentManagerServiceRolePolicy

Deskripsi: Kebijakan ini memberikan izin kepada Manajer Insiden untuk mengelola catatan insiden dan sumber daya terkait atas nama Anda.

`AWSIncidentManagerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 10 Mei 2021, 03:34 UTC
- Waktu teredit: 28 Januari 2025, 02:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "UpdateIncidentRecordPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:CreateTimelineEvent"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RelatedOpsItemPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AssociateOpsItemRelatedItem"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IncidentEngagementPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-contacts:StartEngagement",
      "Resource" : "*"
    },
    {
      "Sid" : "PutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/IncidentManager",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoT1ClickFullAccess

Deskripsi: Menyediakan akses penuh ke AWS IoT 1-Click.

`AWSIoT1ClickFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoT1ClickFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Mei 2018, 22:10 UTC
- Waktu teredit: 11 Mei 2018, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoT1ClickReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke AWS IoT 1-Click.

`AWSIoT1ClickReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoT1ClickReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 11 Mei 2018, 21:49 UTC
- Waktu teredit: 11 Mei 2018, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:Describe*",
        "iot1click:Get*",
        "iot1click:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTAnalyticsFullAccess

Deskripsi: Menyediakan akses penuh ke IoT Analytics.

`AWSIoTAnalyticsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTAnalyticsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Juni 2018, 23:02 UTC
- Waktu teredit: 18 Juni 2018, 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotanalytics:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTAnalyticsReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke IoT Analytics.

`AWSIoTAnalyticsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTAnalyticsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Juni 2018, 21:37 UTC
- Waktu teredit: 18 Juni 2018, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotanalytics:Describe*",
        "iotanalytics:List*",
        "iotanalytics:Get*",
        "iotanalytics:SampleChannelData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTConfigAccess

Deskripsi: Kebijakan ini memberikan akses penuh ke tindakan konfigurasi AWS IoT

`AWSIoTConfigAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTConfigAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Oktober 2015, 21:52 UTC
- Waktu teredit: 27 September 2019, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:AcceptCertificateTransfer",
        "iot:AddThingToThingGroup",
        "iot:AssociateTargetsWithJob",
        "iot:AttachPolicy",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CancelCertificateTransfer",
        "iot:CancelJob",
        "iot:CancelJobExecution",
        "iot:ClearDefaultAuthorizer",
        "iot:CreateAuthorizer",
        "iot:CreateCertificateFromCsr",
        "iot:CreateJob",
        "iot:CreateKeysAndCertificate",
        "iot:CreateOTAUpdate",
        "iot:CreatePolicy",
        "iot:CreatePolicyVersion",
        "iot:CreateRoleAlias",
        "iot:CreateStream",
        "iot:CreateThing",
        "iot:CreateThingGroup",
        "iot:CreateThingType",
        "iot:CreateTopicRule",
        "iot:DeleteAuthorizer",
        "iot:DeleteCACertificate",
        "iot:DeleteCertificate",
        "iot:DeleteJob",
```

```
        "iot:DeleteJobExecution",
        "iot:DeleteOTAUpdate",
        "iot:DeletePolicy",
        "iot:DeletePolicyVersion",
        "iot:DeleteRegistrationCode",
        "iot:DeleteRoleAlias",
        "iot:DeleteStream",
        "iot:DeleteThing",
        "iot:DeleteThingGroup",
        "iot:DeleteThingType",
        "iot:DeleteTopicRule",
        "iot:DeleteV2LoggingLevel",
        "iot:DeprecateThingType",
        "iot:DescribeAuthorizer",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeDefaultAuthorizer",
        "iot:DescribeEndpoint",
        "iot:DescribeEventConfigurations",
        "iot:DescribeIndex",
        "iot:DescribeJob",
        "iot:DescribeJobExecution",
        "iot:DescribeRoleAlias",
        "iot:DescribeStream",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingRegistrationTask",
        "iot:DescribeThingType",
        "iot:DetachPolicy",
        "iot:DetachPrincipalPolicy",
        "iot:DetachThingPrincipal",
        "iot:DisableTopicRule",
        "iot:EnableTopicRule",
        "iot:GetEffectivePolicies",
        "iot:GetIndexingConfiguration",
        "iot:GetJobDocument",
        "iot:GetLoggingOptions",
        "iot:GetOTAUpdate",
        "iot:GetPolicy",
        "iot:GetPolicyVersion",
        "iot:GetRegistrationCode",
        "iot:GetTopicRule",
        "iot:GetV2LoggingOptions",
        "iot:ListAttachedPolicies",
```

```
        "iot:ListAuthorizers",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCertificatesByCA",
        "iot:ListIndices",
        "iot:ListJobExecutionsForJob",
        "iot:ListJobExecutionsForThing",
        "iot:ListJobs",
        "iot:ListOTAUpdates",
        "iot:ListOutgoingCertificates",
        "iot:ListPolicies",
        "iot:ListPolicyPrincipals",
        "iot:ListPolicyVersions",
        "iot:ListPrincipalPolicies",
        "iot:ListPrincipalThings",
        "iot:ListRoleAliases",
        "iot:ListStreams",
        "iot:ListTargetsForPolicy",
        "iot:ListThingGroups",
        "iot:ListThingGroupsForThing",
        "iot:ListThingPrincipals",
        "iot:ListThingRegistrationTaskReports",
        "iot:ListThingRegistrationTasks",
        "iot:ListThings",
        "iot:ListThingsInThingGroup",
        "iot:ListThingTypes",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:RegisterCACertificate",
        "iot:RegisterCertificate",
        "iot:RegisterThing",
        "iot:RejectCertificateTransfer",
        "iot:RemoveThingFromThingGroup",
        "iot:ReplaceTopicRule",
        "iot:SearchIndex",
        "iot:SetDefaultAuthorizer",
        "iot:SetDefaultPolicyVersion",
        "iot:SetLoggingOptions",
        "iot:SetV2LoggingLevel",
        "iot:SetV2LoggingOptions",
        "iot:StartThingRegistrationTask",
        "iot:StopThingRegistrationTask",
        "iot:TestAuthorization",
        "iot:TestInvokeAuthorizer",
```

```
        "iot:TransferCertificate",
        "iot:UpdateAuthorizer",
        "iot:UpdateCACertificate",
        "iot:UpdateCertificate",
        "iot:UpdateEventConfigurations",
        "iot:UpdateIndexingConfiguration",
        "iot:UpdateRoleAlias",
        "iot:UpdateStream",
        "iot:UpdateThing",
        "iot:UpdateThingGroup",
        "iot:UpdateThingGroupsForThing",
        "iot:UpdateAccountAuditConfiguration",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DeleteAccountAuditConfiguration",
        "iot:StartOnDemandAuditTask",
        "iot:CancelAuditTask",
        "iot:DescribeAuditTask",
        "iot:ListAuditTasks",
        "iot:CreateScheduledAudit",
        "iot:UpdateScheduledAudit",
        "iot:DeleteScheduledAudit",
        "iot:DescribeScheduledAudit",
        "iot:ListScheduledAudits",
        "iot:ListAuditFindings",
        "iot:CreateSecurityProfile",
        "iot:DescribeSecurityProfile",
        "iot:UpdateSecurityProfile",
        "iot:DeleteSecurityProfile",
        "iot:AttachSecurityProfile",
        "iot:DetachSecurityProfile",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListActiveViolations",
        "iot:ListViolationEvents",
        "iot:ValidateSecurityProfileBehaviors"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTConfigReadOnlyAccess

Deskripsi: Kebijakan ini memberikan akses baca saja ke tindakan konfigurasi AWS IoT

`AWSIoTConfigReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTConfigReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Oktober 2015, 21:52 UTC
- Waktu teredit: 27 September 2019, 20.52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeAuthorizer",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeDefaultAuthorizer",
        "iot:DescribeEndpoint",
        "iot:DescribeEventConfigurations",
        "iot:DescribeIndex",
        "iot:DescribeJob",
        "iot:DescribeJobExecution",
        "iot:DescribeRoleAlias",
        "iot:DescribeStream",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingRegistrationTask",
        "iot:DescribeThingType",
        "iot:GetEffectivePolicies",
        "iot:GetIndexingConfiguration",
        "iot:GetJobDocument",
        "iot:GetLoggingOptions",
        "iot:GetOTAUpdate",
        "iot:GetPolicy",
        "iot:GetPolicyVersion",
        "iot:GetRegistrationCode",
        "iot:GetTopicRule",
        "iot:GetV2LoggingOptions",
        "iot:ListAttachedPolicies",
        "iot:ListAuthorizers",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCertificatesByCA",
        "iot:ListIndices",
        "iot:ListJobExecutionsForJob",
        "iot:ListJobExecutionsForThing",
        "iot:ListJobs",
        "iot:ListOTAUpdates",
        "iot:ListOutgoingCertificates",
        "iot:ListPolicies",
        "iot:ListPolicyPrincipals",
        "iot:ListPolicyVersions",
        "iot:ListPrincipalPolicies",
        "iot:ListPrincipalThings",
        "iot:ListRoleAliases",
```

```
        "iot:ListStreams",
        "iot:ListTargetsForPolicy",
        "iot:ListThingGroups",
        "iot:ListThingGroupsForThing",
        "iot:ListThingPrincipals",
        "iot:ListThingRegistrationTaskReports",
        "iot:ListThingRegistrationTasks",
        "iot:ListThings",
        "iot:ListThingsInThingGroup",
        "iot:ListThingTypes",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:SearchIndex",
        "iot:TestAuthorization",
        "iot:TestInvokeAuthorizer",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuditTask",
        "iot:ListAuditTasks",
        "iot:DescribeScheduledAudit",
        "iot:ListScheduledAudits",
        "iot:ListAuditFindings",
        "iot:DescribeSecurityProfile",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListActiveViolations",
        "iot:ListViolationEvents",
        "iot:ValidateSecurityProfileBehaviors"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTDataAccess

Deskripsi: Kebijakan ini memberikan akses penuh ke tindakan pesan AWS IoT

`AWSIoTDataAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTDataAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Oktober 2015, 21:51 UTC
- Waktu teredit: 23 Juni 2021, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDataAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:Connect",
        "iot:Publish",
        "iot:Subscribe",
        "iot:Receive",
        "iot:GetThingShadow",
```

```
        "iot:UpdateThingShadow",
        "iot:DeleteThingShadow",
        "iot:ListNamedShadowsForThing"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

Deskripsi: Menyediakan akses tulis ke grup benda IoT dan akses baca ke Sertifikat IoT untuk pelaksanaan tindakan mitigasi ADD_THINGS_TO_THING_GROUP

`AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 Agustus 2019, 17:55 UTC
- Waktu teredit: 07 Agustus 2019, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:ListPrincipalThings",
        "iot:AddThingToThingGroup"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTDeviceDefenderAudit

Deskripsi: Menyediakan akses baca untuk IoT dan sumber daya terkait

`AWSIoTDeviceDefenderAudit`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTDeviceDefenderAudit` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 18 Juli 2018, 21:17 UTC
- Waktu teredit: 25 November 2019, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:GetLoggingOptions",
        "iot:GetV2LoggingOptions",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:ListPolicies",
        "iot:GetPolicy",
        "iot:GetEffectivePolicies",
        "iot:ListRoleAliases",
        "iot:DescribeRoleAlias",
        "cognito-identity:GetIdentityPoolRoles",
```

```
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:GetServiceLastAccessedDetails"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

Deskripsi: Menyediakan akses untuk mengaktifkan pencatatan IoT untuk eksekusi tindakan mitigasi ENABLE_IOT_LOGGING

`AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 07 Agustus 2019, 17:04 UTC
- Waktu teredit: 07 Agustus 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:SetV2LoggingOptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com"
          ]
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

Deskripsi: Menyediakan pesan mempublikasikan akses ke topik SNS untuk eksekusi tindakan mitigasi PUBLISH_FINDING_TO_SNS

`AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 Agustus 2019, 17:04 UTC
- Waktu teredit: 07 Agustus 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

Deskripsi: Menyediakan akses tulis ke kebijakan IoT untuk eksekusi tindakan mitigasi REPLACE_DEFAULT_POLICY_VERSION

`AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 Agustus 2019, 17:04 UTC
- Waktu teredit: 07 Agustus 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:CreatePolicyVersion"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTDeviceDefenderUpdateCACertMitigationAction

Deskripsi: Menyediakan akses tulis ke sertifikat CA IoT untuk eksekusi tindakan mitigasi UPDATE_CA_CERTIFICATE

`AWSIoTDeviceDefenderUpdateCACertMitigationAction`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTDeviceDefenderUpdateCACertMitigationAction` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 Agustus 2019, 17:05 UTC
- Waktu teredit: 07 Agustus 2019, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:UpdateCACertificate"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

Deskripsi: Menyediakan akses tulis ke sertifikat IoT untuk eksekusi tindakan mitigasi UPDATE_DEVICE_CERTIFICATE

`AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 Agustus 2019, 17:06 UTC
- Waktu teredit: 07 Agustus 2019, 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:UpdateCertificate"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTDeviceTesterForFreeRTOSFullAccess

Deskripsi: Mengizinkan AWS IoT Device Tester menjalankan rangkaian kualifikasi FreeRTOS dengan mengizinkan akses ke layanan termasuk IoT, S3, dan IAM

`AWSIoTDeviceTesterForFreeRTOSFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTDeviceTesterForFreeRTOSFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Februari 2020, 20:33 UTC
- Waktu teredit: 10 Agustus 2023, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/idt-*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "iot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteThing",
        "iot:AttachThingPrincipal",
        "iot:DeleteCertificate",
        "iot:GetRegistrationCode",
        "iot:CreatePolicy",
        "iot:UpdateCACertificate",
        "s3:ListBucket",
        "iot:DescribeEndpoint",
        "iot:CreateOTAUpdate",
        "iot:CreateStream",
        "signer:ListSigningJobs",
        "acm:ListCertificates",
        "iot:CreateKeysAndCertificate",
        "iot:UpdateCertificate",
        "iot:CreateCertificateFromCsr",
        "iot:DetachThingPrincipal",
        "iot:RegisterCACertificate",
        "iot:CreateThing",
        "iam:ListRoles",
        "iot:RegisterCertificate",
        "iot:DeleteCACertificate",
        "signer:PutSigningProfile",
        "s3:ListAllMyBuckets",
        "signer:ListSigningPlatforms",
        "iot-device-tester:SendMetrics",
        "iot-device-tester:SupportedVersion",
        "iot-device-tester:LatestIdt",
        "iot-device-tester:CheckVersion",
        "iot-device-tester:DownloadTestSuite"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor2",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "signer:StartSigningJob",
        "acm:GetCertificate",
        "signer:DescribeSigningJob",
        "s3:CreateBucket",
        "execute-api:Invoke",
        "s3:DeleteBucket",
        "s3:PutBucketVersioning",
        "signer:CancelSigningProfile"
      ],
      "Resource" : [
        "arn:aws:execute-api:us-east-1:098862408343:9xpmnvs5h4/prod/POST/metrics",
        "arn:aws:signer:*:*:/signing-profiles/*",
        "arn:aws:signer:*:*:/signing-jobs/*",
        "arn:aws:iam::*:role/idt-*",
        "arn:aws:acm:*:*:certificate/*",
        "arn:aws:s3:::idt-*",
        "arn:aws:s3:::afr-ota*"
      ]
    },
    {
      "Sid" : "VisualEditor3",
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteStream",
        "iot:DeleteCertificate",
        "iot:AttachPolicy",
        "iot:DetachPolicy",
        "iot:DeletePolicy",
        "s3:ListBucketVersions",
        "iot:UpdateCertificate",
        "iot:GetOTAUpdate",
        "iot:DeleteOTAUpdate",
        "iot:DescribeJobExecution"
      ],
      "Resource" : [
        "arn:aws:s3:::afr-ota*",
        "arn:aws:iot:*:*:thinggroup/idt*",
        "arn:aws:iam::*:role/idt-*"
      ]
    },
    {
```

```
      "Sid" : "VisualEditor4",
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteCertificate",
        "iot:AttachPolicy",
        "iot:DetachPolicy",
        "s3:DeleteObjectVersion",
        "iot:DeleteOTAUpdate",
        "s3:PutObject",
        "s3:GetObject",
        "iot:DeleteStream",
        "iot:DeletePolicy",
        "s3:DeleteObject",
        "iot:UpdateCertificate",
        "iot:GetOTAUpdate",
        "s3:GetObjectVersion",
        "iot:DescribeJobExecution"
      ],
      "Resource" : [
        "arn:aws:s3:::afr-ota*/*",
        "arn:aws:s3:::idt-*/*",
        "arn:aws:iot:*:*:policy/idt*",
        "arn:aws:iam::*:role/idt-*",
        "arn:aws:iot:*:*:otaupdate/idt*",
        "arn:aws:iot:*:*:thing/idt*",
        "arn:aws:iot:*:*:cert/*",
        "arn:aws:iot:*:*:job/*",
        "arn:aws:iot:*:*:stream/*"
      ]
    },
    {
      "Sid" : "VisualEditor5",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::afr-ota*/*",
        "arn:aws:s3:::idt-*/*"
      ]
    },
    {
      "Sid" : "VisualEditor6",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iot:CancelJobExecution"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:job/*",
        "arn:aws:iot:*:*:thing/idt*"
      ]
    },
    {
      "Sid" : "VisualEditor7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/Owner" : "IoTDeviceTester"
        }
      }
    },
    {
      "Sid" : "VisualEditor8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/Owner" : "IoTDeviceTester"
        }
      }
    },
    {
      "Sid" : "VisualEditor9",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Owner" : "IoTDeviceTester"
        }
      }
    },
    {
      "Sid" : "VisualEditor10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "VisualEditor11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Owner" : "IoTDeviceTester"
        }
      }
    },
    {
```

```
      "Sid" : "VisualEditor12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ssm:DescribeParameters",
        "ssm:GetParameters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "Owner"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateSecurityGroup"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTDeviceTesterForGreengrassFullAccess

Deskripsi: Memungkinkan AWS IoT Device Tester menjalankan rangkaian kualifikasi AWS Greengrass dengan mengizinkan akses ke layanan terkait termasuk Lambda, IoT, API Gateway, IAM

`AWSIoTDeviceTesterForGreengrassFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTDeviceTesterForGreengrassFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 Februari 2020, 21:21 UTC
- Waktu teredit: 25 Juni 2020, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/idt-*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com",
            "lambda.amazonaws.com",
            "greengrass.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "VisualEditor2",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "iot:DeleteCertificate",
        "lambda:DeleteFunction",
        "execute-api:Invoke",
        "iot:UpdateCertificate"
      ],
      "Resource" : [
        "arn:aws:execute-api:us-east-1:098862408343:9xpmnvs5h4/prod/POST/metrics",
        "arn:aws:lambda:*:*:function:idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "VisualEditor3",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "VisualEditor4",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachPolicy",
        "iot:DetachPolicy",
```

```
        "iot:DeletePolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "VisualEditor5",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateJob",
        "iot:DescribeJob",
        "iot:DescribeJobExecution",
        "iot:DeleteJob"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/idt-*",
        "arn:aws:iot:*:*:job/*"
      ]
    },
    {
      "Sid" : "VisualEditor6",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint",
        "greengrass:*",
        "iam:ListAttachedRolePolicies",
        "iot:CreatePolicy",
        "iot:GetThingShadow",
        "iot:CreateKeysAndCertificate",
        "iot:ListThings",
        "iot:UpdateThingShadow",
        "iot:CreateCertificateFromCsr",
        "iot-device-tester:SendMetrics",
        "iot-device-tester:SupportedVersion",
        "iot-device-tester:LatestIdt",
        "iot-device-tester:CheckVersion",
        "iot-device-tester:DownloadTestSuite"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor7",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iot:DetachThingPrincipal",
        "iot:AttachThingPrincipal"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "VisualEditor8",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:DeleteObjectVersion",
        "s3:ListBucketVersions",
        "s3:CreateBucket",
        "s3:DeleteObject",
        "s3:DeleteBucket"
      ],
      "Resource" : "arn:aws:s3:::idt*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTEventsFullAccess

Deskripsi: Menyediakan akses penuh ke Acara IoT.

`AWSIoTEventsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTEventsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 Januari 2019, 22:51 UTC
- Waktu teredit: 10 Januari 2019, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotevents:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTEventsReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Acara IoT.

`AWSIoTEventsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTEventsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 Januari 2019, 22:50 UTC
- Waktu teredit: 23 September 2019, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iotevents:Describe*",
        "iotevents:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTFleetHubFederationAccess

Deskripsi: Akses federasi untuk aplikasi IoT Fleet Hub

`AWSIoTFleetHubFederationAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTFleetHubFederationAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 15 Desember 2020, 08:08 UTC
- Waktu teredit: 04 April 2022, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTFleetHubFederationAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeIndex",
        "iot:DescribeThingGroup",
        "iot:GetBucketsAggregation",
        "iot:GetCardinality",
        "iot:GetIndexingConfiguration",
        "iot:GetPercentiles",
        "iot:GetStatistics",
        "iot:SearchIndex",
        "iot:CreateFleetMetric",
        "iot:ListFleetMetrics",
        "iot:DeleteFleetMetric",
        "iot:DescribeFleetMetric",
        "iot:UpdateFleetMetric",
        "iot:DescribeCustomMetric",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListMetricValues",
        "iot:ListThingGroups",
        "iot:ListThingsInThingGroup",
        "iot:ListJobTemplates",
        "iot:DescribeJobTemplate",
        "iot:ListJobs",
        "iot:CreateJob",
        "iot:CancelJob",
        "iot:DescribeJob",
        "iot:ListJobExecutionsForJob",
        "iot:ListJobExecutionsForThing",
        "iot:DescribeJobExecution",
        "iot:ListSecurityProfiles",
        "iot:DescribeSecurityProfile",
        "iot:ListActiveViolations",
```

```
        "iot:GetThingShadow",
        "iot:ListNamedShadowsForThing",
        "iot:CancelJobExecution",
        "iot:DescribeEndpoint",
        "iotfleethub:DescribeApplication",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:ListSubscriptionsByTopic",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:iotfleethub*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:iotfleethub*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTFleetwiseServiceRolePolicy

Deskripsi: Memberikan izin ke Sumber AWS Daya dan MetaData yang digunakan atau dikelola oleh AWSIoTFleetwise untuk fitur tambahan

`AWSIoTFleetwiseServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 21 September 2022, 23:27 UTC
- Waktu teredit: 16 Oktober 2025, 04:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTFleetwiseServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/IoTFleetWise",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTFullAccess

Deskripsi: Kebijakan ini memberikan akses penuh ke konfigurasi AWS IoT dan tindakan pengiriman pesan

`AWSIoTFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Oktober 2015, 15:19 UTC
- Waktu teredit: 19 Mei 2022, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:*",
        "iotjobsdata:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTLogging

Deskripsi: Memungkinkan pembuatan CloudWatch grup Amazon Log dan streaming log ke grup

`AWSIoTLogging`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTLogging` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 08 Oktober 2015, 15:17 UTC
- Waktu teredit: 08 Oktober 2015, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTLogging`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy",
        "logs:GetLogEvents",
        "logs:DeleteLogStream"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTManagedIntegrationsFullAccess

Deskripsi: Menyediakan akses penuh ke integrasi terkelola untuk Manajemen Perangkat AWS IoT dan layanan terkait.

`AWSIoTManagedIntegrationsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTManagedIntegrationsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Maret 2025, 19:22 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTManagedIntegrationsFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iotmanagedintegrations:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
iotmanagedintegrations.amazonaws.com/AWSServiceRoleForIoTManagedIntegrations",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "iotmanagedintegrations.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTManagedIntegrationsRolePolicy

Deskripsi: Menyediakan integrasi terkelola untuk izin Manajemen Perangkat AWS IoT untuk menerbitkan log dan metrik atas nama Anda.

`AWSIoTManagedIntegrationsRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 05 Maret 2025, 21:22 UTC
- Waktu teredit: 05 Maret 2025, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTManagedIntegrationsRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/iotmanagedintegrations/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchStreams",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/iotmanagedintegrations/*:log-stream:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/IoTManagedIntegrations",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTOTAUpdate

Deskripsi: Mengizinkan akses untuk membuat Pekerjaan AWS IoT dan menjelaskan pekerjaan penandatangan AWS kode

`AWSIoTOTAUpdate`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTOTAUpdate` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 Desember 2017, 20:36 UTC
- Waktu teredit: 20 Desember 2017, 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTOTAUpdate`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "iot:CreateJob",
      "signer:DescribeSigningJob"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIotRoboRunnerFullAccess

Deskripsi: Kebijakan ini memberikan izin yang memungkinkan akses penuh ke AWS Iot RoboRunner.

`AWSIotRoboRunnerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIotRoboRunnerFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2021, 03:54 UTC
- Waktu teredit: 23 Februari 2023, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIotRoboRunnerFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : "iotroborunner:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/iotroborunner.amazonaws.com/
AWSServiceRoleForIoTRoboRunner",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "iotroborunner.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIotRoboRunnerReadOnly

Deskripsi: Kebijakan ini memberikan izin yang mengizinkan akses baca-saja ke AWS Iot. RoboRunner

`AWSIotRoboRunnerReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIotRoboRunnerReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2021, 03:43 UTC

- Waktu teredit: 16 November 2022, 20.51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIotRoboRunnerReadOnly`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotroborunner:GetSite",
        "iotroborunner:GetWorker",
        "iotroborunner:ListWorkerFleets",
        "iotroborunner:ListSites",
        "iotroborunner:ListWorkers",
        "iotroborunner:GetDestination",
        "iotroborunner:GetWorkerFleet",
        "iotroborunner:ListDestinations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIotRoboRunnerServiceRolePolicy

Deskripsi: AWS Men RoboRunner gizinkan IoT mengelola AWS Sumber Daya terkait atas nama pelanggan.

`AWSIotRoboRunnerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 21 Februari 2023, 16:56 UTC
- Waktu teredit: 21 Februari 2023, 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIotRoboRunnerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
```

```
        "cloudwatch:namespace" : [
          "AWS/Usage"
        ]
      }
    }
  }
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTRuleActions

Deskripsi: Mengizinkan akses ke semua AWS layanan yang didukung dalam Tind AWS akan Aturan IoT

`AWSIoTRuleActions`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTRuleActions` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 08 Oktober 2015, 15:14 UTC
- Waktu teredit: 16 Januari 2018, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "dynamodb:PutItem",
      "kinesis:PutRecord",
      "iot:Publish",
      "s3:PutObject",
      "sns:Publish",
      "sqs:SendMessage*",
      "cloudwatch:SetAlarmState",
      "cloudwatch:PutMetricData",
      "es:ESHttpPut",
      "firehose:PutRecord"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTSiteWiseConsoleFullAccess

Deskripsi: Menyediakan akses penuh untuk mengelola AWS IoT SiteWise menggunakan Konsol Manajemen AWS. Perhatikan bahwa kebijakan ini juga memberikan akses untuk membuat dan membuat daftar penyimpanan data yang digunakan dengan AWS IoT SiteWise (misalnya AWS IoT Analytics), akses ke daftar dan melihat sumber daya AWS IoT Greengrass, membuat daftar dan memodifikasi AWS rahasia Manajer Rahasia, mengambil bayangan benda AWS IoT, mencantumkan sumber daya dengan tag tertentu, dan membuat dan menggunakan peran terkait layanan untuk IoT. AWS SiteWise

`AWSIoTSiteWiseConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTSiteWiseConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 31 Mei 2019, 21:37 UTC
- Waktu teredit: 31 Mei 2019, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "iotsitewise:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iotanalytics:List*",
        "iotanalytics:Describe*",
        "iotanalytics:Create*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
```

```
    },
    {
      "Action" : [
        "iot:DescribeEndpoint",
        "iot:GetThingShadow"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:ListGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "secretsmanager:ListSecrets",
        "secretsmanager:CreateSecret"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "secretsmanager:UpdateSecret"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:greengrass-*"
    },
    {
      "Action" : [
        "tag:GetResources"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/iotsitewise.amazonaws.com/
AWSServiceRoleForIoTSiteWise*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "iotsitewise.amazonaws.com"
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/iotsitewise.amazonaws.com/
AWSServiceRoleForIoTSiteWise*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "iotsitewise.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTSiteWiseFullAccess

Deskripsi: Menyediakan akses penuh ke IoT SiteWise.

`AWSIoTSiteWiseFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTSiteWiseFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Desember 2018, 20:53 UTC
- Waktu teredit: 04 Desember 2018, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTSiteWiseMonitorPortalAccess

Deskripsi: Kebijakan ini memberikan izin untuk mengakses SiteWise aset AWS IoT dan data aset, membuat sumber daya AWS IoT SiteWise Monitor, dan membuat daftar pengguna AWS SSO.

`AWSIoTSiteWiseMonitorPortalAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTSiteWiseMonitorPortalAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Mei 2020, 20:01 UTC
- Waktu teredit: 19 Mei 2020, 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:CreateProject",
        "iotsitewise:DescribeProject",
        "iotsitewise:UpdateProject",
        "iotsitewise:DeleteProject",
        "iotsitewise:ListProjects",
        "iotsitewise:BatchAssociateProjectAssets",
        "iotsitewise:BatchDisassociateProjectAssets",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:CreateDashboard",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:UpdateDashboard",
        "iotsitewise:DeleteDashboard",
        "iotsitewise:ListDashboards",
        "iotsitewise:CreateAccessPolicy",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:UpdateAccessPolicy",
        "iotsitewise:DeleteAccessPolicy",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:DescribeAsset",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:GetAssetPropertyValue",
        "iotsitewise:GetAssetPropertyValueHistory",
        "iotsitewise:GetAssetPropertyAggregates",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTSiteWiseMonitorServiceRolePolicy

Deskripsi: Peran ini memberikan izin SiteWise monitor AWS IoT untuk mengakses SiteWise aset & properti aset AWS IoT Anda, dan membuat proyek AWS IoT Sitewise, dasbor & kebijakan akses melalui portal AWS IoT SiteWise .

`AWSIoTSiteWiseMonitorServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 14 November 2019, 00:59 UTC
- Waktu teredit: 13 Desember 2019, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:CreateProject",
```

```
        "iotsitewise:DescribeProject",
        "iotsitewise:UpdateProject",
        "iotsitewise:DeleteProject",
        "iotsitewise:ListProjects",
        "iotsitewise:BatchAssociateProjectAssets",
        "iotsitewise:BatchDisassociateProjectAssets",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:CreateDashboard",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:UpdateDashboard",
        "iotsitewise:DeleteDashboard",
        "iotsitewise:ListDashboards",
        "iotsitewise:CreateAccessPolicy",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:UpdateAccessPolicy",
        "iotsitewise:DeleteAccessPolicy",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:DescribeAsset",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:GetAssetPropertyValue",
        "iotsitewise:GetAssetPropertyValueHistory",
        "iotsitewise:GetAssetPropertyAggregates",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTSiteWiseReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke IoT SiteWise.

`AWSIoTSiteWiseReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTSiteWiseReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Desember 2018, 20:55 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:BatchGetAssetPropertyAggregates",
        "iotsitewise:BatchGetAssetPropertyValue",
        "iotsitewise:BatchGetAssetPropertyValueHistory",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAction",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetCompositeModel",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeAssetModelCompositeModel",
        "iotsitewise:DescribeAssetModelInterfaceRelationship",
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:DescribeBulkImportJob",
        "iotsitewise:DescribeComputationModel",
```

```
        "iotsitewise:DescribeComputationModelExecutionSummary",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeDataset",
        "iotsitewise:DescribeDefaultEncryptionConfiguration",
        "iotsitewise:DescribeExecution",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribeGatewayCapabilityConfiguration",
        "iotsitewise:DescribeLoggingOptions",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:DescribeStorageConfiguration",
        "iotsitewise:DescribeTimeSeries",
        "iotsitewise:ExecuteQuery",
        "iotsitewise:GetAssetPropertyAggregates",
        "iotsitewise:GetAssetPropertyValue",
        "iotsitewise:GetAssetPropertyValueHistory",
        "iotsitewise:GetInterpolatedAssetPropertyValues",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListActions",
        "iotsitewise:ListAssetModelCompositeModels",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:ListAssetRelationships",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:ListBulkImportJobs",
        "iotsitewise:ListCompositionRelationships",
        "iotsitewise:ListComputationModelDataBindingUsages",
        "iotsitewise:ListComputationModelResolveToResources",
        "iotsitewise:ListComputationModels",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListDatasets",
        "iotsitewise:ListExecutions",
        "iotsitewise:ListGateways",
        "iotsitewise:ListInterfaceRelationships",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iotsitewise:ListTimeSeries"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTThingsRegistration

Deskripsi: Kebijakan ini memungkinkan pengguna mendaftarkan barang secara massal menggunakan AWS IoT StartThingRegistrationTask API

`AWSIoTThingsRegistration`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTThingsRegistration` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Desember 2017, 20:21 UTC
- Waktu teredit: 05 Oktober 2020 19.20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:AddThingToThingGroup",
        "iot:AttachPolicy",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CreateCertificateFromCsr",
        "iot:CreatePolicy",
        "iot:CreateThing",
        "iot:DescribeCertificate",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:DetachPolicy",
        "iot:DetachThingPrincipal",
        "iot:GetPolicy",
        "iot:ListAttachedPolicies",
        "iot:ListPolicyPrincipals",
        "iot:ListPrincipalPolicies",
        "iot:ListPrincipalThings",
        "iot:ListTargetsForPolicy",
        "iot:ListThingGroupsForThing",
        "iot:ListThingPrincipals",
        "iot:RegisterCertificate",
        "iot:RegisterThing",
        "iot:RemoveThingFromThingGroup",
        "iot:UpdateCertificate",
        "iot:UpdateThing",
        "iot:UpdateThingGroupsForThing",
        "iot:AddThingToBillingGroup",
        "iot:DescribeBillingGroup",
        "iot:RemoveThingFromBillingGroup"
      ],
      "Resource" : [
        "*"
      ]
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTTwinMakerServiceRolePolicy

Deskripsi: Men AWS giz TwinMaker inkan IoT memanggil AWS layanan lain dan menyinkronkan sumber daya mereka atas nama Anda.

`AWSIoTTwinMakerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 13 November 2023, 18:59 UTC
- Waktu teredit: 13 November 2023, 18.59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTTwinMakerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SiteWiseAssetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:DescribeAsset"
      ],
      "Resource" : [
        "arn:aws:iotsitewise:*:*:asset/*"
      ]
    },
    {
      "Sid" : "SiteWiseAssetModelReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:DescribeAssetModel"
      ],
      "Resource" : [
        "arn:aws:iotsitewise:*:*:asset-model/*"
      ]
    },
    {
      "Sid" : "SiteWiseAssetModelAndAssetListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssetModels"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TwinMakerAccess",
      "Effect" : "Allow",
      "Action" : [
        "iottwinmaker:GetEntity",
        "iottwinmaker:CreateEntity",
        "iottwinmaker:UpdateEntity",
```

```
        "iottwinmaker:DeleteEntity",
        "iottwinmaker:ListEntities",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:CreateComponentType",
        "iottwinmaker:UpdateComponentType",
        "iottwinmaker:DeleteComponentType",
        "iottwinmaker:ListComponentTypes"
      ],
      "Resource" : [
        "arn:aws:iottwinmaker:*:*:workspace/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iottwinmaker:linkedServices" : [
            "IOTSITEWISE"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTWirelessDataAccess

Deskripsi: Mengizinkan akses data identitas terkait ke perangkat AWS IoT Wireless.

`AWSIoTWirelessDataAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTWirelessDataAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Desember 2020, 15:31 UTC

- Waktu teredit: 15 Desember 2020, 15:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotwireless:SendDataToWirelessDevice"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTWirelessFullAccess

Deskripsi: Mengizinkan akses penuh identitas terkait ke semua operasi AWS IoT Wireless.

`AWSIoTWirelessFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTWirelessFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Desember 2020, 15:27 UTC
- Waktu teredit: 15 Desember 2020, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotwireless:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTWirelessFullPublishAccess

Deskripsi: Menyediakan akses penuh IoT Wireless untuk menerbitkan ke IoT Rules Engine atas nama Anda.

`AWSIoTWirelessFullPublishAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTWirelessFullPublishAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Desember 2020, 15:29 UTC
- Waktu teredit: 15 Desember 2020, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iot:DescribeEndpoint",
        "iot:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTWirelessGatewayCertManager

Deskripsi: Mengizinkan akses identitas terkait untuk membuat, membuat daftar, dan menjelaskan Sertifikat IoT

`AWSIoTWirelessGatewayCertManager`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTWirelessGatewayCertManager` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Desember 2020, 15:30 UTC
- Waktu teredit: 15 Desember 2020, 15.30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IoTWirelessGatewayCertManager",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:DescribeCertificate",
        "iot:ListCertificates"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTWirelessLogging

Deskripsi: Mengizinkan identitas terkait untuk membuat grup Amazon CloudWatch Logs dan melakukan streaming log ke grup.

`AWSIoTWirelessLogging`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTWirelessLogging` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Desember 2020, 15:32 UTC
- Waktu teredit: 15 Desember 2020, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessLogging`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotwireless*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIoTWirelessReadOnlyAccess

Deskripsi: Mengizinkan akses baca saja identitas terkait ke AWS IoT nirkabel.

`AWSIoTWirelessReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIoTWirelessReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Desember 2020, 15:28 UTC
- Waktu teredit: 15 Desember 2020, 15:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotwireless:List*",
```

```
        "iotwireless:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIPAMServiceRolePolicy

Deskripsi: Mengizinkan VPC IP Address Manager mengakses sumber daya VPC dan berintegrasi dengan AWS Organisasi atas nama Anda.

`AWSIPAMServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 30 November 2021, 19:08 UTC
- Waktu teredit: 09 September 2026, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IPAMDiscoveryDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredPublicAddresses",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "ec2:GetIpamDiscoveredRoutes",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListByoipCidrs",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit",
        "cloudfront:ListAnycastIpLists",
        "cloudfront:ListDistributionsByAnycastIpListId",
        "cloudfront:ListTagsForResource"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "CloudWatchMetricsPublishActions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/IPAM"
        }
      }
    },
    {
      "Sid" : "IPAMAllocationPolicyActions",
      "Effect" : "Allow",
      "Action" : "ec2:AllocateIpamPoolCidr",
      "Resource" : "*"
    },
    {
      "Sid" : "PrefixListResolverWriteActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyManagedPrefixList"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "ec2:Attribute/ExpectedIpamPrefixListResolverTarget" : "false"
        }
      }
    },
    {
      "Sid" : "PrefixListResolverReadActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIQContractServiceRolePolicy

Deskripsi: Digunakan oleh AWS IQ untuk mengeksekusi permintaan pembayaran atas nama pelanggan

`AWSIQContractServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 22 Agustus 2019, 19:28 UTC
- Waktu teredit: 22 Agustus 2019, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:Subscribe"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIQFullAccess

Deskripsi: Menyediakan akses penuh ke AWS IQ

`AWSIQFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIQFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 April 2019, 23:13 UTC
- Waktu teredit: 25 September 2019, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIQFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iq:*",
        "iq-permission:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "permission.iq.amazonaws.com",
            "contract.iq.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSIQPermissionServiceRolePolicy

Deskripsi: Memungkinkan AWS IQ untuk mengelola peran yang diasumsikan oleh para ahli AWS IQ.

`AWSIQPermissionServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 22 Agustus 2019, 19:36 UTC
- Waktu teredit: 22 Agustus 2019, 19.36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQPermissionServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:ListAttachedRolePolicies"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/AWSDenyAll"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

Deskripsi: Mengaktifkan akses ke AWS layanan dan sumber daya yang diperlukan untuk penyimpanan kunci kustom AWS KMS

`AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 14 November 2018, 20:10 UTC
- Waktu teredit: 10 November 2023, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:Describe*",
        "ec2:CreateNetworkInterface",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

Deskripsi: Mengaktifkan AWS KMS untuk menyinkronkan properti bersama dari kunci Multi-wilayah.

`AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 16 Juni 2021, 15:37 UTC
- Waktu teredit: 13 November 2024, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "KMSSynchronizeMultiRegionKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:SynchronizeMultiRegionKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSKeyManagementServicePowerUser

Deskripsi: Menyediakan akses ke AWS Key Management Service (KMS).

`AWSKeyManagementServicePowerUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSKeyManagementServicePowerUser` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 07 Maret 2017, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSKeyManagementServicePowerUser`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateAlias",
        "kms:CreateKey",
        "kms:DeleteAlias",
        "kms:Describe*",
        "kms:GenerateRandom",
        "kms:Get*",
        "kms:List*",
        "kms:TagResource",
        "kms:UntagResource",
        "iam:ListGroups",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLakeFormationCrossAccountManager

Deskripsi: Menyediakan akses lintas akun ke sumber daya Glue melalui Formasi Danau. Juga memberikan akses baca ke layanan lain yang diperlukan seperti organisasi dan manajer akses sumber daya

`AWSLakeFormationCrossAccountManager`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLakeFormationCrossAccountManager` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Agustus 2020, 20:59 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManageResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:GetResourceShares"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManageResourceSharePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceSharePermission"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "AllowXAcctManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:PutResourcePolicy",
        "glue:DeleteResourcePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "ram:Get*",
        "ram:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLakeFormationDataAdmin

Deskripsi: Memberikan akses administratif ke Formasi AWS Danau dan layanan terkait, seperti AWS Glue, untuk mengelola danau data

`AWSLakeFormationDataAdmin`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLakeFormationDataAdmin` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Agustus 2019, 17:33 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSLakeFormationDataAdminAllow",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "glue:CreateCatalog",
        "glue:UpdateCatalog",
        "glue:DeleteCatalog",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:CreateDatabase",
```

```
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:GetConnections",
        "glue:SearchTables",
        "glue:GetTable",
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue:DeleteTable",
        "glue:GetTableVersions",
        "glue:GetPartitions",
        "glue:GetTables",
        "glue:ListWorkflows",
        "glue:BatchGetWorkflows",
        "glue:DeleteWorkflow",
        "glue:GetWorkflowRuns",
        "glue:StartWorkflowRun",
        "glue:GetWorkflow",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "iam:ListUsers",
        "iam:ListRoles",
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSLakeFormationDataAdminDeny",
      "Effect" : "Deny",
      "Action" : [
        "lakeformation:PutDataLakeSettings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWS Lambda_FullAccess

Deskripsi: Memberikan akses penuh ke layanan AWS Lambda, fitur konsol AWS Lambda, dan layanan terkait AWS lainnya.

`AWSLambda_FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambda_FullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 November 2020, 21:14 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_FullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
```

```
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "lambda:*",
        "logs:DescribeLogGroups",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "tag:GetResources",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/lambda.amazonaws.com/
AWSServiceRoleForLambda",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lambda.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWS Lambda_ReadOnlyAccess

Deskripsi: Memberikan akses baca-saja ke layanan AWS Lambda, fitur konsol AWS Lambda, dan layanan terkait lainnya. AWS

`AWSLambda_ReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambda_ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 November 2020, 21:10 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "lambda:Get*",
        "lambda:List*",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "tag:GetResources",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:DescribeQueries",
        "logs:GetLogGroupFields",
        "logs:GetLogRecord",
        "logs:GetQueryResults",
        "logs:StartLiveTail",
        "logs:StopLiveTail"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLambdaBasicDurableExecutionRolePolicy

Deskripsi: Memberikan izin menulis ke CloudWatch Log dan read/write izin ke API eksekusi tahan lama yang digunakan oleh fungsi tahan lama Lambda

`AWSLambdaBasicDurableExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaBasicDurableExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 02 Desember 2025, 15:04 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaBasicDurableExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "lambda:CheckpointDurableExecution",
        "lambda:GetDurableExecutionState"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLambdaBasicExecutionRole

Deskripsi: Menyediakan izin menulis ke CloudWatch Log.

`AWSLambdaBasicExecutionRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaBasicExecutionRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 09 April 2015, 15:03 UTC
- Waktu teredit: 09 April 2015, 15:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
```

```
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLambdaDynamoDBExecutionRole

Deskripsi: Menyediakan akses daftar dan baca ke aliran DynamoDB dan izin menulis ke CloudWatch log.

`AWSLambdaDynamoDBExecutionRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaDynamoDBExecutionRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 09 April 2015, 15:09 UTC
- Waktu teredit: 09 April 2015, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLambdaENIManagementAccess

Deskripsi: Memberikan izin minimum untuk fungsi Lambda untuk mengelola ENI (membuat, menjelaskan, menghapus) yang digunakan oleh Fungsi VPC-enabled Lambda.

`AWSLambdaENIManagementAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaENIManagementAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Desember 2016, 00:37 UTC
- Waktu teredit: 01 Oktober 2020, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLambdaExecute

> **Important**
>
> Kebijakan `AWSLambdaExecute` terkelola sedang menuju penghentian, dan tidak lagi direkomendasikan untuk digunakan dengan AWS Lambda. Sebaliknya, gunakan `AWSLambdaBasicExecutionRole`. Ketika layanan IAM akhirnya menghentikan kebijakan tersebut, Anda tidak akan dapat melampirkannya ke peran. Namun, Anda dapat melampirkan peran yang ada ke sumber daya meskipun peran tersebut menggunakan kebijakan yang tidak digunakan lagi.

Deskripsi: Menyediakan Put, Dapatkan akses ke S3 dan akses penuh ke CloudWatch Log.

`AWSLambdaExecute`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaExecute` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaExecute`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:*"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLambdaFullAccess

Deskripsi: Kebijakan ini berada di jalur penghentian. Lihat dokumentasi untuk panduan: Men https://docs.aws.amazon.com/lambda/latest/dg/access-control-identity-based.html. yediakan akses penuh ke Lambda, S3, DynamoDB, CloudWatch Metrik dan Log.

`AWSLambdaFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 27 November 2017, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaFullAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
```

```
        "cloudwatch:*",
        "cognito-identity:ListIdentityPools",
        "cognito-sync:GetCognitoEvents",
        "cognito-sync:SetCognitoEvents",
        "dynamodb:*",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "events:*",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:PassRole",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy",
        "iot:CreateThing",
        "iot:CreateTopicRule",
        "iot:DescribeEndpoint",
        "iot:GetTopicRule",
        "iot:ListPolicies",
        "iot:ListThings",
        "iot:ListTopicRules",
        "iot:ReplaceTopicRule",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "kinesis:PutRecord",
        "kms:ListAliases",
        "lambda:*",
        "logs:*",
        "s3:*",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Publish",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sqs:ListQueues",
        "sqs:SendMessage",
```

```
        "tag:GetResources",
        "xray:PutTelemetryRecords",
        "xray:PutTraceSegments"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLambdaInvocation-DynamoDB

Deskripsi: Menyediakan akses baca ke Streams DynamoDB.

`AWSLambdaInvocation-DynamoDB`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaInvocation-DynamoDB` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 06 Februari 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLambdaInvokeWebFunctionEndpointAccess

Deskripsi: Memberikan izin untuk memanggil titik akhir fungsi AWS Lambda Web.

`AWSLambdaInvokeWebFunctionEndpointAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaInvokeWebFunctionEndpointAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Oktober 2026, 16:47 UTC
- Waktu teredit: 01 Oktober 2026, 16:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaInvokeWebFunctionEndpointAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeWebFunctionEndpoint"
      ],
      "Resource" : "arn:aws:lambda:*:*:web-function/*/endpoint/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLambdaKinesisExecutionRole

Deskripsi: Menyediakan akses daftar dan baca ke aliran Kinesis dan izin menulis ke CloudWatch log.

`AWSLambdaKinesisExecutionRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaKinesisExecutionRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 09 April 2015, 15:14 UTC
- Waktu teredit: 19 November 2018, 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary",
        "kinesis:GetRecords",
        "kinesis:GetShardIterator",
        "kinesis:ListShards",
        "kinesis:ListStreams",
        "kinesis:SubscribeToShard",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLambdaManagedEC2ResourceOperator

Deskripsi: Kebijakan ini memberikan izin untuk membuat dan mengelola sumber daya EC2 yang dikelola oleh Instans Terkelola Lambda, dan izin deskriptif.

`AWSLambdaManagedEC2ResourceOperator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaManagedEC2ResourceOperator` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2025, 08:34 UTC
- Waktu teredit: 10 Juni 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaManagedEC2ResourceOperator`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateTags",
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "scaler.lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEncryptionControls"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : "amazon"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*:log-stream:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLambdaMSKExecutionRole

Deskripsi: Menyediakan izin yang diperlukan untuk mengakses Cluster MSK dalam VPC, mengelola ENI (membuat, menjelaskan, menghapus) di VPC dan menulis izin ke Log. CloudWatch

`AWSLambdaMSKExecutionRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaMSKExecutionRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 Agustus 2020, 17:35 UTC
- Waktu teredit: 02 Agustus 2022, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaMSKExecutionRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:GetBootstrapBrokers",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLambdaNetworkConnectorOperatorPolicy

Deskripsi: Kebijakan ini memberikan izin untuk membuat dan mengelola sumber daya ENI yang dikelola oleh Konektor Jaringan Lambda

`AWSLambdaNetworkConnectorOperatorPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaNetworkConnectorOperatorPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 Juni 2026, 15:27 UTC
- Waktu teredit: 22 Juni 2026, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaNetworkConnectorOperatorPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateEniInAnySubnet",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:subnet/*"
```

```
    },
    {
      "Sid" : "AllowCreateEniWithSecurityGroups",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "AllowCreateEniWithLambdaTagKeys",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:lambda:networkConnectorName",
            "aws:lambda:networkConnectorId"
          ]
        }
      }
    },
    {
      "Sid" : "TagENIOnCreate",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface",
          "ec2:ManagedResourceOperator" : "network-connectors.lambda.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLambdaReplicator

Deskripsi: Memberikan izin yang diperlukan Lambda Replicator untuk mereplikasi fungsi di seluruh wilayah

`AWSLambdaReplicator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 23 Mei 2017, 17:53 UTC
- Waktu teredit: 08 Desember 2017, 00:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LambdaCreateDeletePermission",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:DisableReplication"
      ],
```

```
      "Resource" : [
        "arn:aws:lambda:*:*:function:*"
      ]
    },
    {
      "Sid" : "IamPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFrontListDistributions",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributionsByLambdaFunction"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLambdaRole

Deskripsi: Kebijakan default untuk peran layanan AWS Lambda.

`AWSLambdaRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 06 Februari 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLambdaServiceRolePolicy

Deskripsi: Mengizinkan Lambda menjelaskan dan menghentikan instans terkelola dari EC2 atas nama Anda.

`AWSLambdaServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 30 November 2025, 08:04 UTC
- Waktu teredit: 22 Juni 2026, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "scaler.lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "network-connectors.lambda.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLambdaSQSQueueExecutionRole

Deskripsi: Menyediakan pesan terima, menghapus pesan, dan membaca akses atribut ke antrian SQS, dan izin menulis ke CloudWatch log.

`AWSLambdaSQSQueueExecutionRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaSQSQueueExecutionRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Juni 2018, 21:50 UTC
- Waktu teredit: 14 Juni 2018, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLambdaVPCAccessExecutionRole

Deskripsi: Memberikan izin minimum untuk fungsi Lambda untuk dijalankan saat mengakses sumber daya dalam VPC - membuat, menjelaskan, menghapus antarmuka jaringan, dan menulis izin ke CloudWatch Log.

`AWSLambdaVPCAccessExecutionRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaVPCAccessExecutionRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 11 Februari 2016, 23:15 UTC
- Waktu teredit: 05 Januari 2024, 22:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSLambdaVPCAccessExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLicenseManagerConsumptionPolicy

Deskripsi: Menyediakan izin untuk mengiz AWS inkan akses ke tindakan API Manajer Lisensi yang diperlukan untuk menggunakan lisensi yang memiliki hak pengguna.

`AWSLicenseManagerConsumptionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLicenseManagerConsumptionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 Agustus 2021, 23:18 UTC
- Waktu teredit: 11 Agustus 2021, 23:18 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
```

```
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

Deskripsi: Mengizinkan Layanan Langganan Linux Manajer AWS Lisensi untuk mengelola sumber daya atas nama Anda.

`AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 20 Desember 2022, 18:54 UTC
- Waktu teredit: 08 Juli 2024, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LicenseManagerLinuxSubscriptions" : "enabled",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*"
      ]
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LicenseManagerLinuxSubscriptions" : "enabled",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLicenseManagerMasterAccountRolePolicy

Deskripsi: Kebijakan peran akun master layanan Manajer AWS Lisensi

`AWSLicenseManagerMasterAccountRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 26 November 2018, 19:03 UTC
- Waktu teredit: 31 Mei 2022, 20:50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
```

```
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "S3ObjectPermissions1",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "S3ObjectPermissions2",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*/resource_sync/*"
      ]
    },
    {
      "Sid" : "AthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StartQueryExecution"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "GluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTable",
        "glue:GetPartition",
        "glue:GetPartitions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RAMPermissions1",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareAssociations",
        "ram:TagResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RAMPermissions2",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ram:CreateResourceShare"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Service" : "LicenseManager"
        }
      }
    },
    {
      "Sid" : "RAMPermissions3",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Service" : "LicenseManager"
        }
      }
    },
    {
      "Sid" : "IAMGetRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMPassRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/LicenseManagerServiceResourceDataSyncRole*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "cloudformation.amazonaws.com",
            "glue.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudformationPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/
LicenseManagerCrossAccountCloudDiscoveryStack/*"
      ]
    },
    {
      "Sid" : "GlueUpdatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue:DeleteTable",
        "glue:UpdateJob",
        "glue:UpdateCrawler"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:crawler/LicenseManagerResourceSynDataCrawler",
        "arn:aws:glue:*:*:job/LicenseManagerResourceSynDataProcessJob",
        "arn:aws:glue:*:*:table/license_manager_resource_inventory_db/*",
        "arn:aws:glue:*:*:table/license_manager_resource_sync/*",
        "arn:aws:glue:*:*:database/license_manager_resource_inventory_db",
```

```
        "arn:aws:glue:*:*:database/license_manager_resource_sync"
      ]
    },
    {
      "Sid" : "RGPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:PutGroupPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLicenseManagerMemberAccountRolePolicy

Deskripsi: Kebijakan peran akun anggota layanan Manajer AWS Lisensi

`AWSLicenseManagerMemberAccountRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran

- Waktu pembuatan: 26 November 2018, 19:04 UTC
- Waktu teredit: 15 November 2019, 22:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LicenseManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "license-manager:UpdateLicenseSpecificationsForResource",
        "license-manager:GetLicenseConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListInventoryEntries",
        "ssm:GetInventory",
        "ssm:CreateAssociation",
        "ssm:CreateResourceDataSync",
        "ssm:DeleteResourceDataSync",
        "ssm:ListResourceDataSync",
        "ssm:ListAssociations"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RAMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourceShareInvitations"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLicenseManagerServiceRolePolicy

Deskripsi: Kebijakan peran default layanan Manajer AWS Lisensi

`AWSLicenseManagerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 26 November 2018, 19:02 UTC
- Waktu teredit: 19 November 2025, 18:34 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/license-
management.marketplace.amazonaws.com/AWSServiceRoleForMarketplaceLicenseManagement"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "license-management.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPermissionsForCreatingMemberSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/aws-service-role/license-manager.member-
account.amazonaws.com/AWSServiceRoleForAWSLicenseManagerMemberAccountRole"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "license-manager.member-account.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3BucketPermissions1",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "S3BucketPermissions2",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3ObjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "SNSAccountPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
```

```
        "arn:aws:sns:*:*:aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "SNSTopicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeHosts"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListInventoryEntries",
        "ssm:GetInventory",
        "ssm:CreateAssociation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMSendCommandPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*::document/AWSLicenseManager-*"
      ]
    },
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "LicenseManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "license-manager:GetServiceSettings",
        "license-manager:GetLicense*",
        "license-manager:UpdateLicenseSpecificationsForResource",
        "license-manager:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

Deskripsi: Mengizinkan Layanan Langganan Pengguna Manajer AWS Lisensi untuk mengelola sumber daya atas nama Anda.

`AWSLicenseManagerUserSubscriptionsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 30 Juli 2022, 01:17 UTC
- Waktu teredit: 10 Juli 2026, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
```

```
        "ds:GetAuthorizedApplicationDetails",
        "ds:DescribeTrusts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetInventory",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVpcPeeringConnections"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2WritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CreateTags"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:productCode" : [
            "bz0vcy31ooqlzk5tsash4r1ik",
            "d44g89hc0gp9jdzm99rznthpw",
            "77yzkpa7kvee1y1tt7wnsdwoc",
            "a8jthu9h8pjsn4b8ylvfl6sfr",
            "7at6der8hnlov1g347e6tdkde",
            "3t0v0vuhvxjzm6m462f9v8iz4",
            "4gs2prcp03ojilgkjx8m3ifh7",
            "5uypd9kpy863kwykrwn4bcolv",
            "eqtok9gt75we12qgk28b955qc"
```

```
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "SSMDocumentExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunPowerShellScript"
      ]
    },
    {
      "Sid" : "SSMInstanceExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSLicenseManager" : "UserSubscriptions"
        }
      }
    },
    {
      "Sid" : "ReadHostedZonePermissions",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListResourceRecordSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadSecurityGroupRulePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeSecurityGroupRules"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Sid" : "DescribeSubnetsPermissions",
      "Action" : [
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeNetworkInterfacePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadSecretPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:license-manager-user-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSM2ServicePolicy

Deskripsi: Men AWS gizinkan M2 mengelola AWS sumber daya atas nama Anda.

`AWSM2ServicePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 07 Juni 2022, 20:26 UTC
- Waktu teredit: 07 Juni 2022, 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/M2"
          ]
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSManagedAccountManagementAccess

Deskripsi: Memberikan AWS izin untuk memperbarui dan memelihara peran ter AWS kelola untuk akun AWS terkelola

`AWSManagedAccountManagementAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSManagedAccountManagementAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 Juli 2026, 19:57 UTC
- Waktu teredit: 01 Oktober 2026, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedAccountManagementAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:TagRole",
        "iam:UntagRole",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole"
      ],
      "Resource" : "arn:*:iam::*:role/managed/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:*:iam::*:role/managed/AWSManagedAccountManagementAccessRole",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSManagedAccountUserEntitlementAccess

Deskripsi: Mem AWS berikan izin untuk mengelola hak akses akun untuk akun terkel AWS ola

`AWSManagedAccountUserEntitlementAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSManagedAccountUserEntitlementAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: Juli 17, 2026, 21:42 UTC
- Waktu teredit: 17 Juli 2026, 21:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedAccountUserEntitlementAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "identitystore:CreateGroup",
      "identitystore:GetGroupId",
      "identitystore:GetUserId",
      "identitystore:CreateGroupMembership",
      "sso:ListInstances",
```

```
      "sso-directory:ListProvisioningTenants",
      "account-access:ListApplications",
      "account-access:CreateEntitlement",
      "account-access:ListEntitlements"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSManagedAdvancedFeaturesActivationAccess

Deskripsi: Memberikan AWS izin untuk mengaktifkan fitur lanjutan untuk akun AWS terkelola

`AWSManagedAdvancedFeaturesActivationAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSManagedAdvancedFeaturesActivationAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Juli 2026, 14:27 UTC
- Waktu teredit: 21 Juli 2026, 14:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedAdvancedFeaturesActivationAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "iam:PutAccountProperties"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSManagedBudgetsSpendLimitManagementAccess

Deskripsi: Memberikan izin layanan Anggaran untuk melampirkan dan melepaskan Kebijakan Kontrol Layanan dan mengelola akun di AWS Organisasi untuk menerapkan pag AWS ar pembatas pengeluaran pada akun anggota.

`AWSManagedBudgetsSpendLimitManagementAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSManagedBudgetsSpendLimitManagementAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Juli 2026, 21:12 UTC
- Waktu teredit: 07 Agustus 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedBudgetsSpendLimitManagementAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SCPActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:AttachPolicy",
        "organizations:DescribePolicy",
        "organizations:DetachPolicy"
      ],
      "Resource" : "arn:aws:organizations::*:policy/*/service_control_policy/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ManagedBy" : "SpendLimit"
        }
      }
    },
    {
      "Sid" : "SCPListPolicyAction",
      "Effect" : "Allow",
      "Action" : "organizations:ListPolicies",
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "SCPTargetActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:AttachPolicy",
        "organizations:DetachPolicy"
      ],
      "Resource" : "arn:aws:organizations::*:account/*"
    },
    {
      "Sid" : "AccountActions",
      "Effect" : "Allow",
      "Action" : "organizations:CloseAccount",
      "Resource" : "arn:aws:organizations::*:account/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSManagedControlPolicyManagementAccess

Deskripsi: Mem AWS berikan izin untuk mengelola kebijakan kontrol organisasi untuk akun ter AWS kelola

`AWSManagedControlPolicyManagementAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSManagedControlPolicyManagementAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Juli 2026, 14:27 UTC
- Waktu teredit: 21 Juli 2026, 14:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedControlPolicyManagementAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribePolicy",
      "organizations:UpdatePolicy",
      "organizations:ListPolicies",
      "organizations:ListRoots",
      "organizations:CreatePolicy",
      "organizations:AttachPolicy",
      "organizations:DetachPolicy",
      "organizations:DeletePolicy",
      "organizations:TagResource",
      "organizations:UntagResource",
      "organizations:ListTagsForResource"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSManagedServiceAccessManagementAccess

Deskripsi: Memberikan izin untuk mengelola Kebijakan Kontrol Layanan (SCP) di AWS Organisasi untuk layanan Manajemen Ak AWS ses Layanan Terkelola. Termasuk izin untuk membuat daftar, membuat, memperbarui, dan melampirkan SCP yang dicakup ke kebijakan yang ditandai dengan ManagedBy =service-access.

`AWSManagedServiceAccessManagementAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSManagedServiceAccessManagementAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 21 Juli 2026, 17:57 UTC
- Waktu teredit: 21 Juli 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSManagedServiceAccessManagementAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowListRoots",
      "Effect" : "Allow",
      "Action" : "organizations:ListRoots",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSCPList",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : "SERVICE_CONTROL_POLICY"
        }
      }
    },
    {
      "Sid" : "AllowSCPCreateWithTag",
      "Effect" : "Allow",
      "Action" : [
        "organizations:CreatePolicy",
        "organizations:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : "SERVICE_CONTROL_POLICY",
          "aws:RequestTag/ManagedBy" : "service-access"
        }
      }
    },
    {
      "Sid" : "AllowSCPUpdateTagged",
      "Effect" : "Allow",
```

```
      "Action" : "organizations:UpdatePolicy",
      "Resource" : "arn:aws:organizations::*:policy/*/service_control_policy/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ManagedBy" : "service-access"
        }
      }
    },
    {
      "Sid" : "AllowSCPAttachTaggedPolicy",
      "Effect" : "Allow",
      "Action" : "organizations:AttachPolicy",
      "Resource" : "arn:aws:organizations::*:policy/*/service_control_policy/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ManagedBy" : "service-access"
        }
      }
    },
    {
      "Sid" : "AllowSCPAttachRoot",
      "Effect" : "Allow",
      "Action" : "organizations:AttachPolicy",
      "Resource" : "arn:aws:organizations::*:root/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSManagedServices_ContactsServiceRolePolicy

Deskripsi: AWS Mengizinkan Layanan Terkelola membaca nilai tag pada AWS sumber daya

`AWSManagedServices_ContactsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 23 Maret 2023, 17:07 UTC
- Waktu teredit: 23 Maret 2023, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_ContactsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoleTags",
        "iam:ListUserTags",
        "tag:GetResources",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetBucketTagging",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:authType" : "REST-HEADER",
          "s3:signatureversion" : "AWS4-HMAC-SHA256"
        },
        "NumericGreaterThanEquals" : {
          "s3:TlsVersion" : "1.2"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

Deskripsi: AWS Layanan Terkelola - kebijakan untuk mengelola infrastruktur kontrol detektif

`AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 19 Desember 2022, 23:11 UTC
- Waktu teredit: 19 Desember 2022, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateTermination*",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackResources",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplateSummary",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/ams-detective-controls-config-recorder",
        "arn:aws:cloudformation:*:*:stack/ams-detective-controls-config-rules-cdk",
        "arn:aws:cloudformation:*:*:stack/ams-detective-controls-infrastructure-cdk"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeAggregationAuthorizations",
        "config:PutAggregationAuthorization",
        "config:TagResource",
        "config:PutConfigRule"
      ],
      "Resource" : [
        "arn:aws:config:*:*:aggregation-authorization/540708452589/*",
        "arn:aws:config:*:*::config-rule/*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketPolicy",
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetBucketAcl",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:PutBucketLogging",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::ams-config-record-bucket-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSManagedServices_EventsServiceRolePolicy

Deskripsi: AWS Kebijakan Layanan Terkelola untuk mengaktifkan fitur prosesor acara AMS.

`AWSManagedServices_EventsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 07 Februari 2023, 18:41 UTC
- Waktu teredit: 07 Februari 2023, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "events.managedservices.amazonaws.com"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSManagedServices_SelfServiceReporting_ServiceRolePolicy

Deskripsi: Mengizinkan fitur Pelaporan Layanan Mandiri Amazon Man AWS aged Service membaca data AWS Organisasi atas nama Anda untuk mengaktifkan pelaporan agregat tingkat organisasi

`AWSManagedServices_SelfServiceReporting_ServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 08 Januari 2025, 21:22 UTC
- Waktu teredit: 08 Januari 2025, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_SelfServiceReporting_ServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSManagedServicesDeploymentToolkitPolicy

Deskripsi: Mengiz AWS inkan Layanan Terkelola mengelola toolkit penerapan atas nama Anda.

`AWSManagedServicesDeploymentToolkitPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 09 Juni 2022, 18:33 UTC
- Waktu teredit: 04 April 2024, 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AMSCDKToolkitS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObject",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersion",
        "s3:DeleteObjectVersionTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
```

```
        "s3:GetBucketVersioning",
        "s3:GetLifecycleConfiguration",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectAttributes",
        "s3:GetObjectLegalHold",
        "s3:GetObjectRetention",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionAttributes",
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionTorrent",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutBucketAcl",
        "s3:PutBucketLogging",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::ams-cdktoolkit*"
    },
    {
      "Sid" : "AMSCDKToolkitCloudFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplate",
        "cloudformation:GetTemplateSummary",
        "cloudformation:TagResource",
        "cloudformation:UntagResource",
```

```
        "cloudformation:UpdateTerminationProtection"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*"
    },
    {
      "Sid" : "AMSCDKToolkitECRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:CreateRepository",
        "ecr:DeleteLifecyclePolicy",
        "ecr:DeleteRepository",
        "ecr:DeleteRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:ListTagsForResource",
        "ecr:PutImageScanningConfiguration",
        "ecr:PutImageTagMutability",
        "ecr:PutLifecyclePolicy",
        "ecr:SetRepositoryPolicy",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/ams-cdktoolkit*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSManagedSettingsAdminAccess

Deskripsi: Memberikan akses administratif penuh ke manajemen Akun AWS pengaturan. Kebijakan ini memungkinkan pemilik untuk melihat dan mengubah informasi akun, penagihan, pembayaran, pendaftaran pajak, manajemen identitas, kebijakan organisasi, anggaran, analisis biaya, dan pemberitahuan ruang kerja. Ditujukan untuk pemilik ruang kerja yang membutuhkan akses administratif lengkap atas konfigurasi akun dan manajemen anggota. Kebijakan ini tidak memberikan

akses ke layanan komputasi, penyimpanan, jaringan, atau infrastruktur lain yang tidak terkait dengan pengaturan akun.

`AWSManagedSettingsAdminAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSManagedSettingsAdminAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: Juli 22, 2026, 01:27 UTC
- Waktu teredit: 30 September 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedSettingsAdminAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ActivateAdvancedUpdateAccountName",
      "Effect" : "Allow",
      "Action" : [
        "account:PutAccountName"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "account.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "AWSSettingsAccountAccess",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetContactInformation",
        "account:CloseAccount",
        "account:PutAccountName",
        "account:PutContactInformation",
        "account:StartPrimaryEmailUpdate",
        "account:AcceptPrimaryEmailUpdate",
        "account:GetPrimaryEmailUpdateStatus",
        "account:SendPhoneNumberVerification",
        "account:VerifyPhoneNumber",
        "notifications:AssociateManagedNotificationAccountContact",
        "notifications:DisassociateManagedNotificationAccountContact",
        "notifications:ListManagedNotificationChannelAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsBillingAccess",
      "Effect" : "Allow",
      "Action" : [
        "billing:GetCredits",
        "billing:GetSellerOfRecord",
        "billing:RedeemCredits"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsCostExplorerAccess",
      "Effect" : "Allow",
      "Action" : [
        "ce:GetCostAndUsage",
        "ce:GetCostForecast"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsBudgetsAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "budgets:CreateBudgetAction",
        "budgets:DeleteBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ModifyBudget",
        "budgets:ViewBudget",
        "budgets:UpdateBudget",
        "budgets:CreateBudget",
        "budgets:DeleteBudget",
        "budgets:DescribeBudgets",
        "budgets:DescribeBudget",
        "budgets:DescribeBudgetActionHistories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsIAMPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/managed/
AWSManagedBudgetsSpendLimitManagementRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "budgets.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSettingsCustomerVerificationAccess",
      "Effect" : "Allow",
      "Action" : [
        "customer-verification:CreateCustomerVerificationDetails",
        "customer-verification:CreateUploadUrls",
        "customer-verification:GetCustomerVerificationDetails",
        "customer-verification:GetCustomerVerificationEligibility",
        "customer-verification:UpdateCustomerVerificationDetails",
        "customer-verification:GetInheritanceConfig",
        "customer-verification:PutInheritanceConfig"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AWSSettingsFreeTierAccess",
      "Effect" : "Allow",
      "Action" : [
        "freetier:GetAccountPlanState",
        "freetier:UpgradeAccountPlan"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsIdentityStoreAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:CreateGroup",
        "identitystore:CreateGroupMembership",
        "identitystore:CreateUser",
        "identitystore:DeleteGroup",
        "identitystore:DeleteGroupMembership",
        "identitystore:DeleteUser",
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:GetGroupId",
        "identitystore:GetUserId",
        "identitystore:ListGroupMemberships",
        "identitystore:UpdateIdentityStore",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "identitystore:ListUsers",
        "identitystore:ReserveUser",
        "identitystore:UpdateGroup",
        "identitystore:UpdateUser",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchGroups",
        "sso-directory:SearchUsers",
        "builderid:CreateInvitation",
        "builderid:DeleteInvitation",
        "builderid:DisassociateCollaborator",
        "builderid:ListInvitations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsInvoicingAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "invoicing:GetInvoicePDF"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:CloseAccount",
        "organizations:CreatePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:CreateBuilderIdOwnedAccount",
        "organizations:DescribeCreateAccountStatus",
        "organizations:DescribeAccount",
        "organizations:InviteAccountToOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsOrganizationsAiOptOutPolicyManagement",
      "Effect" : "Allow",
      "Action" : [
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:EnablePolicyType",
        "organizations:DisablePolicyType"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : "AISERVICES_OPT_OUT_POLICY"
        }
      }
    },
    {
      "Sid" : "AWSSettingsPaymentsAccess",
      "Effect" : "Allow",
      "Action" : [
        "payments:CreatePaymentInstrument",
```

```
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentPreferences",
        "payments:MakePayment",
        "payments:UpdatePaymentInstrument",
        "payments:UpdatePaymentPreferences",
        "payments:TagResource",
        "payments:UntagResource",
        "payments:ListTagsForResource",
        "payments:BatchGetPaymentProfiles",
        "payments:AcceptTermsAndConditionsForProgramByAccountId",
        "payments:CreatePaymentAttempt",
        "payments:CreatePaymentProfile",
        "payments:Get",
        "payments:GetAcceptedTermsAndConditionsForProgramByAccountId",
        "payments:GetEligibleCurrencies",
        "payments:GetPaymentAttempt",
        "payments:GetPaymentPreferences",
        "payments:GetPreferredCurrency",
        "payments:GetRecommendedTermsAndConditionsForProgram",
        "payments:ListPaymentProfiles",
        "payments:SearchFinancialRecords",
        "payments:SetPreferredCurrency",
        "payments:UpdatePaymentProfile",
        "payments:GetAccountBalance",
        "payments:GetDefaultPaymentProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsSESAccess",
      "Effect" : "Allow",
      "Action" : [
        "ses:SendEmail"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsSSOAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:DeleteApplicationAssignment",
        "sso:DescribeInstance",
        "sso:GetApplicationAssignmentConfiguration",
```

```
        "sso:ListApplicationAssignments",
        "sso:CreateApplicationAssignment",
        "sso:DescribeApplication",
        "sso:ListApplications",
        "sso:UpdateInstance"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsTaxAccess",
      "Effect" : "Allow",
      "Action" : [
        "tax:BatchPutTaxRegistration",
        "tax:DeleteTaxRegistration",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
        "tax:PutTaxRegistration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsSupportAccess",
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeCases",
        "support:AddCommunicationToCase",
        "support:ResolveCase",
        "supportplans:GetSupportPlan",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:GetSupportPlanUpdateStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ActivateAdvancedProvisioningAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:CreateBuilderIdOwnedAccount",
        "organizations:DescribeCreateAccountStatus",
        "organizations:ListAccounts",
```

```
        "sso:ListInstances",
        "identitystore:GetUserId",
        "sso-directory:ListProvisioningTenants",
        "account-access:ListApplications",
        "account-access:CreateApplication",
        "account-access:CreateEntitlement",
        "signin:DeleteConsoleAuthorizationConfiguration",
        "signin:DeleteResourcePermissionStatement",
        "signin:ListResourcePermissionStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "account.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ActivateAdvancedDelegatedAdminAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "account.amazonaws.com",
          "organizations:ServicePrincipal" : [
            "sso.amazonaws.com",
            "account-access.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ActivateAdvancedManagedRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:ListAttachedRolePolicies",
```

```
        "iam:DetachRolePolicy",
        "iam:ListRolePolicies",
        "iam:DeleteRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/managed/*",
        "arn:aws:iam::*:role/ManagedAccountAdmin",
        "arn:aws:iam::*:role/AccountFullAccessRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "account.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ActivateAdvancedMemberAccountAssume",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/managed/
AWSManagedAdvancedFeaturesActivationRole",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "account.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ActivateAdvancedBudgetsAccess",
      "Effect" : "Allow",
      "Action" : "budgets:ModifyBudget",
      "Resource" : "arn:aws:budgets::*:budget/sla-*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "account.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ActivateAdvancedSCPCleanupAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DeletePolicy",
        "organizations:DetachPolicy",
```

```
        "organizations:AttachPolicy",
        "organizations:CreatePolicy",
        "organizations:ListPolicies",
        "organizations:ListRoots"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "account.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceAccessForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "cost-optimization-hub.bcm.amazonaws.com",
            "compute-optimizer.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForComputeOptimizerAutomation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/aco-automation.amazonaws.com/
AWSServiceRoleForComputeOptimizerAutomation",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "aco-automation.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForComputeOptimizer",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/compute-
optimizer.amazonaws.com/AWSServiceRoleForComputeOptimizer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "compute-optimizer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cost-optimization-
hub.bcm.amazonaws.com/AWSServiceRoleForCostOptimizationHub",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cost-optimization-hub.bcm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GetAndUpdateEnrollmentStatusForACOCOH",
      "Effect" : "Allow",
      "Action" : [
        "aco-automation:GetEnrollmentConfiguration",
        "aco-automation:UpdateEnrollmentConfiguration",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:UpdateEnrollmentStatus",
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:UpdateEnrollmentStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSManagedSettingsReadOnlyAccess

Deskripsi: Memberi anggota tim akses baca-saja ke Peng AWS aturan, termasuk ruang kerja dan informasi pemilik, keanggotaan tim, rencana, dan ringkasan pengeluaran. Itu tidak memberikan izin untuk mengubah konfigurasi ruang kerja atau untuk mengelola penagihan dan pembayaran.

`AWSManagedSettingsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSManagedSettingsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: Juli 22, 2026, 01:12 UTC
- Waktu teredit: 21 Agustus 2026, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedSettingsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccountReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetContactInformation"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "IdentityStoreReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroups",
        "identitystore:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeInstance"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSODirectoryReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchGroups",
        "sso-directory:SearchUsers"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSManagedSignUpAdminAccess

Deskripsi: Mem AWS berikan izin untuk menyelesaikan pendaftaran akun AWS terkelola.

`AWSManagedSignUpAdminAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSManagedSignUpAdminAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 Juli 2026, 19:27 UTC
- Waktu teredit: 20 Juli 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSManagedSignUpAdminAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PaymentWidgetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "payments:CreatePaymentInstrument",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentPreferences",
        "payments:ListTagsForResource",
        "payments:MakePayment",
        "payments:TagResource",
        "payments:UntagResource",
        "payments:UpdatePaymentInstrument",
        "payments:UpdatePaymentPreferences"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BillingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "billing:GetSellerOfRecord"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccountPermissions",
      "Effect" : "Allow",
      "Action" : [
        "account:GetContactInformation"
      ],
      "Resource" : "arn:aws:account::*:account"
    },
    {
      "Sid" : "InvoicingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "invoicing:GetInvoicePDF"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "TaxWidgetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tax:BatchPutTaxRegistration",
        "tax:DeleteTaxRegistration",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
        "tax:PutTaxRegistration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CustomerVerificationWidgetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "customer-verification:CreateCustomerVerificationDetails",
        "customer-verification:CreateUploadUrls",
        "customer-verification:GetCustomerVerificationDetails",
        "customer-verification:GetCustomerVerificationEligibility",
        "customer-verification:UpdateCustomerVerificationDetails"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSManagementConsoleAdministratorAccess

Deskripsi: Menyediakan akses penuh untuk mengkonfigurasi dan menyesuaikan Konsol Manajemen AWS

`AWSManagementConsoleAdministratorAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSManagementConsoleAdministratorAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan fungsi pekerjaan
- Waktu pembuatan: 14 Agustus 2025, 21:19 UTC
- Waktu teredit: 23 Maret 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AWSManagementConsoleAdministratorAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "uxc:GetAccountColor",
        "uxc:PutAccountColor",
        "uxc:DeleteAccountColor",
        "uxc:GetAccountCustomizations",
        "uxc:UpdateAccountCustomizations",
        "uxc:ListServices",
        "ec2:DescribeRegions",
        "notifications:GetFeatureOptInStatus",
        "notifications:AssociateChannel",
        "notifications:AssociateManagedNotificationAccountContact",
        "notifications:AssociateManagedNotificationAdditionalChannel",
```

```
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:DeleteEventRule",
        "notifications:DeleteNotificationConfiguration",
        "notifications:DeregisterNotificationHub",
        "notifications:DisableNotificationsAccessForOrganization",
        "notifications:DisassociateChannel",
        "notifications:DisassociateManagedNotificationAccountContact",
        "notifications:DisassociateManagedNotificationAdditionalChannel",
        "notifications:EnableNotificationsAccessForOrganization",
        "notifications:GetEventRule",
        "notifications:GetManagedNotificationChildEvent",
        "notifications:GetManagedNotificationConfiguration",
        "notifications:GetManagedNotificationEvent",
        "notifications:GetNotificationConfiguration",
        "notifications:GetNotificationEvent",
        "notifications:GetNotificationsAccessForOrganization",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListManagedNotificationChildEvents",
        "notifications:ListManagedNotificationConfigurations",
        "notifications:ListManagedNotificationEvents",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationEvents",
        "notifications:ListNotificationHubs",
        "notifications:ListTagsForResource",
        "notifications:RegisterNotificationHub",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "cloudshell:CreateEnvironment",
        "cloudshell:CreateSession",
        "cloudshell:GetEnvironmentStatus",
        "cloudshell:DeleteEnvironment",
        "cloudshell:GetFileDownloadUrls",
        "cloudshell:GetFileUploadUrls",
        "cloudshell:DescribeEnvironments",
        "cloudshell:PutCredentials",
        "cloudshell:StartEnvironment",
        "cloudshell:StopEnvironment",
        "cloudshell:ApproveCommand",
        "q:StartConversation",
```

```
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:PassRequest",
        "resource-explorer-2:AssociateDefaultView",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:CreateView",
        "resource-explorer-2:DeleteIndex",
        "resource-explorer-2:DeleteView",
        "resource-explorer-2:DisassociateDefaultView",
        "resource-explorer-2:GetAccountLevelServiceConfiguration",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetManagedView",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListIndexesForMembers",
        "resource-explorer-2:ListManagedViews",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-explorer-2:Search",
        "resource-explorer-2:TagResource",
        "resource-explorer-2:UntagResource",
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:UpdateView",
        "action-recommendations:ListRecommendedActions",
        "account:GetAccountInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSManagementConsoleBasicUserAccess

Deskripsi: Memberikan akses ke Konsol Manajemen AWS fitur penting dan kemampuan pengalaman pengguna (UX) untuk pengguna non-administratif.

`AWSManagementConsoleBasicUserAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSManagementConsoleBasicUserAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Agustus 2025, 20:34 UTC
- Waktu teredit: 17 Maret 2026, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagementConsoleBasicUserAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "uxc:GetAccountColor",
        "uxc:GetAccountCustomizations",
```

```
        "uxc:ListServices",
        "ec2:DescribeRegions",
        "notifications:GetFeatureOptInStatus",
        "notifications:ListManagedNotificationEvents",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationEvents",
        "notifications:ListNotificationHubs",
        "notifications:GetManagedNotificationChildEvent",
        "notifications:GetManagedNotificationEvent",
        "notifications:GetNotificationEvent",
        "notifications:ListManagedNotificationChildEvents",
        "cloudshell:CreateEnvironment",
        "cloudshell:CreateSession",
        "cloudshell:GetEnvironmentStatus",
        "cloudshell:StartEnvironment",
        "cloudshell:DeleteEnvironment",
        "cloudshell:PutCredentials",
        "cloudshell:StopEnvironment",
        "cloudshell:ApproveCommand",
        "q:StartConversation",
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:PassRequest",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search",
        "action-recommendations:ListRecommendedActions",
        "account:GetAccountInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMarketplaceAmiIngestion

Deskripsi: Memungkinkan AWS Marketplace untuk menyalin Gambar Mesin Amazon Anda (AMI) untuk mencantumkannya di AWS Marketplace

`AWSMarketplaceAmiIngestion`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceAmiIngestion` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 September 2020, 20:55 UTC
- Waktu teredit: 25 September 2020, 20.55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:ec2:us-east-1::snapshot/snap-*"
    },
    {
```

```
      "Action" : [
        "ec2:DescribeImageAttribute",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshotAttribute",
        "ec2:ModifyImageAttribute"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMarketplaceDeploymentServiceRolePolicy

Deskripsi: AWS Marketplace Memungkinkan untuk membuat dan mengelola parameter penerapan penjual untuk produk yang Anda berlangganan AWS Marketplace.

`AWSMarketplaceDeploymentServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 15 November 2023, 23:34 UTC
- Waktu teredit: 15 November 2023, 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageMarketplaceDeploymentSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:RemoveRegionsFromReplication"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:marketplace-deployment*!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "TagMarketplaceDeploymentSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:marketplace-deployment!*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/expirationDate" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "expirationDate"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMarketplaceDiscoveryFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Marketplace Discovery API untuk mencari dan mengambil informasi produk dan harga.

`AWSMarketplaceDiscoveryFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceDiscoveryFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Mei 2026, 17:12 UTC
- Waktu teredit: 07 Mei 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceDiscoveryFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetListing",
        "aws-marketplace:GetProduct",
        "aws-marketplace:GetOffer",
        "aws-marketplace:GetOfferTerms",
        "aws-marketplace:GetOfferSet",
        "aws-marketplace:ListPurchaseOptions",
        "aws-marketplace:ListFulfillmentOptions",
        "aws-marketplace:SearchListings",
        "aws-marketplace:SearchFacets"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/product/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/listing/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/offer/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/offerSet/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/purchaseOption/*"
      ]
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMarketplaceFullAccess

Deskripsi: Menyediakan kemampuan untuk berlangganan dan berhenti berlangganan AWS Marketplace perangkat lunak, memungkinkan pengguna mengelola instans perangkat lunak Marketplace dari halaman 'Perangkat Lunak Anda' Marketplace, dan menyediakan akses administratif ke EC2.

`AWSMarketplaceFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Februari 2015, 17:21 UTC
- Waktu teredit: 11 September 2026, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceFullAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:List*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeAddresses",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcs",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "license-manager:ListReceivedLicenses",
        "payments:ListPaymentProgramStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CopyImage",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:CreateImage",
        "ec2:DescribeInstanceStatus",
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:DescribeDocument",
        "sns:ListTopics",
        "sns:GetTopicAttributes",
        "sns:CreateTopic",
        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:ListRoles",
        "iam:ListInstanceProfiles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "signin:CreateOAuth2Token",
      "Resource" : "arn:aws:signin:*:*:service-principal/marketplace-
mcp.amazonaws.com",
      "Condition" : {
        "StringEquals" : {
          "signin:OAuthGrantType" : "client_credentials"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMarketplaceGetEntitlements

Deskripsi: Menyediakan akses baca ke H AWS Marketplace ak

`AWSMarketplaceGetEntitlements`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceGetEntitlements` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Maret 2017, 19:37 UTC
- Waktu teredit: 05 April 2024, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSMarketplaceGetEntitlements",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetEntitlements"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMarketplaceImageBuildFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Marketplace Fitur Pembuatan Gambar Pribadi. Selain membuat gambar pribadi, ia juga memberikan izin untuk menambahkan tag ke gambar, meluncurkan dan mengakhiri instance ec2.

`AWSMarketplaceImageBuildFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceImageBuildFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 31 Juli 2018, 23:29 UTC
- Waktu teredit: 04 Maret 2022, 17.05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListBuilds",
        "aws-marketplace:StartBuild",
        "aws-marketplace:DescribeBuilds"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/marketplace-image-build:build-id" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*Automation*",
        "arn:aws:iam::*:role/*Instance*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:DescribeDocument",
        "ec2:DeregisterImage",
        "ec2:CopyImage",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DeleteSnapshot",
        "ec2:CreateImage",
        "ec2:RunInstances",
        "ec2:DescribeInstanceStatus",
        "sns:GetTopicAttributes",
```

```
        "iam:GetRole",
        "iam:GetInstanceProfile"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*image-build*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*image-build*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
        "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
        "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
        "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
```

```
        "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
        "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
        "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
        "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
            "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
            "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
            "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
            "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
            "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
            "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
            "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/marketplace-image-build:build-id" : "*"
        },
```

```
        "StringNotEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMarketplaceLicenseManagementServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh AWS Marketplace untuk manajemen lisensi.

`AWSMarketplaceLicenseManagementServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 03 Desember 2020, 08:33 UTC
- Waktu teredit: 03 Desember 2020, 08:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowLicenseManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "license-manager:ListReceivedGrants",
        "license-manager:ListDistributedGrants",
        "license-manager:GetGrant",
        "license-manager:CreateGrant",
        "license-manager:CreateGrantVersion",
        "license-manager:DeleteGrant",
        "license-manager:AcceptGrant"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMarketplaceManageSubscriptions

Deskripsi: Menyediakan kemampuan untuk berlangganan dan berhenti berlangganan AWS Marketplace perangkat lunak

`AWSMarketplaceManageSubscriptions`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceManageSubscriptions` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 07 Mei 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetListing",
        "aws-marketplace:GetProduct",
        "aws-marketplace:GetOffer",
        "aws-marketplace:GetOfferTerms",
        "aws-marketplace:GetOfferSet",
        "aws-marketplace:ListPurchaseOptions",
        "aws-marketplace:ListFulfillmentOptions",
        "aws-marketplace:SearchFacets",
        "aws-marketplace:SearchListings"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/product/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/listing/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/offer/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/offerSet/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/purchaseOption/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:UpdatePurchaseOrders",
        "aws-marketplace:ListAgreementCharges",
        "aws-marketplace:GetAgreementPaymentRequest",
```

```
        "aws-marketplace:ListAgreementPaymentRequests",
        "aws-marketplace:AcceptAgreementPaymentRequest",
        "aws-marketplace:RejectAgreementPaymentRequest"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        },
        "Null" : {
          "aws-marketplace:AgreementType" : "false"
        }
      }
    },
    {
      "Sid" : "AWSMarketplaceChangeSetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
    },
    {
      "Sid" : "AWSMarketplaceTokenManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/AgentTokenContainer/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : [
            "CreateAgentTokenContainer",
            "RequestExpressPrivateOffer",
            "ExpireToken"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "AWSMarketplaceEntityReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceAgreementCancellationRequestAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListAgreementCancellationRequests",
        "aws-marketplace:GetAgreementCancellationRequest",
        "aws-marketplace:AcceptAgreementCancellationRequest",
        "aws-marketplace:CancelAgreement",
        "aws-marketplace:RejectAgreementCancellationRequest"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        },
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Acceptor"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMarketplaceMeteringFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Marketplace Metering.

`AWSMarketplaceMeteringFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceMeteringFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Maret 2016, 22:39 UTC
- Waktu teredit: 17 Maret 2016, 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:MeterUsage"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMarketplaceMeteringRegisterUsage

Deskripsi: Memberikan izin untuk mendaftarkan sumber daya dan melacak penggunaan melalui AWS Marketplace Layanan Pengukuran.

`AWSMarketplaceMeteringRegisterUsage`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceMeteringRegisterUsage` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 November 2019, 01:17 UTC
- Waktu teredit: 21 November 2019, 01:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:RegisterUsage"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMarketplaceProcurementSystemAdminFullAccess

Deskripsi: Menyediakan akses penuh ke semua tindakan administratif untuk integrasi AWS Marketplace eProcurement.

`AWSMarketplaceProcurementSystemAdminFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceProcurementSystemAdminFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Juni 2019, 13:07 UTC

- Waktu teredit: 21 April 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceProcurementSystemAdminFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*",
        "invoicing:CreateProcurementPortalPreference",
        "invoicing:GetProcurementPortalPreference",
        "invoicing:ListProcurementPortalPreferences"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMarketplacePurchaseOrdersServiceRolePolicy

Deskripsi: Mengaktifkan akses AWS Marketplace layanan ke manajemen pesanan pembelian.

`AWSMarketplacePurchaseOrdersServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 27 Oktober 2021, 15:12 UTC
- Waktu teredit: 27 Oktober 2021, 15.12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplacePurchaseOrdersServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPurchaseOrderActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMarketplaceRead-only

Deskripsi: Menyediakan kemampuan untuk meninjau AWS Marketplace langganan

`AWSMarketplaceRead-only`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceRead-only` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 07 Mei 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceRead-only`

Versi kebijakan

Versi kebijakan: v13 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:ListAgreementCharges",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:ListInstanceProfiles",
        "sns:GetTopicAttributes",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests",
        "aws-marketplace:GetAgreementPaymentRequest",
        "aws-marketplace:ListAgreementPaymentRequests"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetListing",
        "aws-marketplace:GetProduct",
        "aws-marketplace:GetOffer",
        "aws-marketplace:GetOfferTerms",
        "aws-marketplace:GetOfferSet",
        "aws-marketplace:ListPurchaseOptions",
        "aws-marketplace:ListFulfillmentOptions",
        "aws-marketplace:SearchFacets",
        "aws-marketplace:SearchListings"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/product/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/listing/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/offer/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/offerSet/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/purchaseOption/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListAgreementCancellationRequests",
        "aws-marketplace:GetAgreementCancellationRequest"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMarketplaceResaleAuthorizationServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh AWS Marketplace untuk Otorisasi Penjualan Kembali.

`AWSMarketplaceResaleAuthorizationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 05 Maret 2024, 18:47 UTC
- Waktu teredit: 01 Agustus 2025, 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceResaleAuthorizationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMCreate",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ram:RequestedResourceType" : "aws-marketplace:Entity"
        },
        "ArnLike" : {
          "ram:ResourceArn" : "arn:aws:aws-marketplace:*:*:*/ResaleAuthorization/*"
        },
        "Null" : {
          "ram:Principal" : "true"
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMAssociate",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "Null" : {
          "ram:Principal" : "false"
        },
        "StringEquals" : {
          "ram:ResourceShareName" : "AWSMarketplaceResaleAuthorization"
        }
      }
```

```
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMAcceptDelete",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:DeleteResourceShare"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ram:ResourceShareName" : "AWSMarketplaceResaleAuthorization"
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMGet",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ]
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsMarketplace",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:*/ResaleAuthorization/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsMarketplaceDescribe",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:*/ResaleAuthorization/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMarketplaceSellerFullAccess

Deskripsi: Menyediakan akses penuh ke semua operasi penjual pada AWS Marketplace dan AWS layanan lainnya seperti manajemen AMI.

`AWSMarketplaceSellerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceSellerFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Juli 2019, 20:40 UTC
- Waktu teredit: 12 Agustus 2026, 16:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess`

Versi kebijakan

Versi kebijakan: v33 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MarketplaceManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace-management:uploadFiles",
        "aws-marketplace-management:viewReports",
        "aws-marketplace-management:viewSupport",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:GetSellerDashboard",
        "aws-marketplace:ListAssessments",
        "aws-marketplace:DescribeAssessment",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:ModifyImageAttribute",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AgreementAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:DescribeAgreement",
        "aws-marketplace:GetAgreementTerms"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        },
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "IAMGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "AssetScanning",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "assets.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VendorInsights",
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*",
        "arn:aws:aws-marketplace:*:*:catalog/AWSMarketplace*/*",
        "arn:aws:aws-marketplace:*:*:verification-type/*/verification-evidence/*",
        "arn:aws:aws-marketplace:*:*:tax-compliance-profile/*",
        "arn:aws:aws-marketplace:*:*:tax-compliance-profile-change-task/*"
      ]
    },
    {
      "Sid" : "SellerSettings",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace-management:GetSellerVerificationDetails",
        "aws-marketplace-management:PutSellerVerificationDetails",
        "aws-marketplace-management:GetBankAccountVerificationDetails",
        "aws-marketplace-management:PutBankAccountVerificationDetails",
        "aws-marketplace-management:GetSecondaryUserVerificationDetails",
        "aws-marketplace-management:PutSecondaryUserVerificationDetails",
        "aws-marketplace-management:GetAdditionalSellerNotificationRecipients",
        "aws-marketplace-management:PutAdditionalSellerNotificationRecipients",
        "payments:GetPaymentInstrument",
        "payments:CreatePaymentInstrument",
        "payments:DeletePaymentInstrument",
        "tax:GetTaxInterview",
        "tax:PutTaxInterview",
        "tax:GetTaxInfoReportingDocument",
        "tax:ListSupplementalTaxRegistrations",
        "tax:PutSupplementalTaxRegistration",
        "tax:DeleteSupplementalTaxRegistration",
        "tax:GetTaxRegistration",
        "tax:PutTaxRegistration",
        "tax:ListTaxRegistrations",
        "aws-marketplace:ListPayables",
```

```
        "aws-marketplace:ListInvoiceSubmissionTasks",
        "invoicing:ListInvoiceSummaries",
        "invoicing:GetInvoicePDF",
        "aws-marketplace:ListIssuedTaxInvoices"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceSellerVerificationEvidenceManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreateVerificationEvidence",
        "aws-marketplace:UpdateVerificationEvidence",
        "aws-marketplace:GetVerificationEvidence"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:verification-type/*/verification-
evidence/*"
    },
    {
      "Sid" : "MarketplaceSellerVerificationManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListVerificationEvidence",
        "aws-marketplace:StartVerification",
        "aws-marketplace:GetVerification",
        "aws-marketplace:ListVerifications"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "InvoiceSubmissionManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartInvoiceSubmissionTask",
        "aws-marketplace:GetInvoiceSubmissionTask"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:catalog/AWSMarketplace*/invoice-
submission-task/*"
    },
    {
      "Sid" : "MarketplaceEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-files/
${aws:PrincipalAccount}/*"
      ]
    },
    {
      "Sid" : "Support",
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourcePolicyManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*",
        "arn:aws:aws-marketplace:*:*:catalog/AWSMarketplace*/*"
      ]
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "resale-authorization.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AgreementPaymentRequestAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SendAgreementPaymentRequest",
        "aws-marketplace:GetAgreementPaymentRequest",
```

```
        "aws-marketplace:ListAgreementPaymentRequests",
        "aws-marketplace:CancelAgreementPaymentRequest"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        },
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VerificationAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:StartVerification",
        "partnercentral:GetVerification"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SellerSettingsGetIssuedTaxInvoice",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetIssuedTaxInvoice"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:catalog/AWSMarketplace*/issued-tax-
invoice/*"
```

```
    },
    {
      "Sid" : "AWSMarketplaceAgreementsCancellationAndAdjustmentAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListAgreementInvoiceLineItems",
        "aws-marketplace:ListBillingAdjustmentRequests",
        "aws-marketplace:GetBillingAdjustmentRequest",
        "aws-marketplace:BatchCreateBillingAdjustmentRequest",
        "aws-marketplace:ListAgreementCancellationRequests",
        "aws-marketplace:GetAgreementCancellationRequest",
        "aws-marketplace:SendAgreementCancellationRequest",
        "aws-marketplace:CancelAgreementCancellationRequest"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        },
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "TaxComplianceProfileChangeTaskManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartTaxComplianceProfileChangeTask"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:tax-compliance-profile-change-task/*"
    },
    {
      "Sid" : "TaxComplianceProfileRead",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetTaxComplianceProfile"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:tax-compliance-profile/*"
    },
    {
      "Sid" : "TaxComplianceProfileList",
```

```
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListTaxComplianceProfileChangeTasks",
        "aws-marketplace:ListTaxComplianceProfiles"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMarketplaceSellerOfferManagement

Deskripsi: Menyediakan akses penjual ke aktivitas manajemen Penawaran dan Perjanjian.

`AWSMarketplaceSellerOfferManagement`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceSellerOfferManagement` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 November 2024, 00:41 UTC
- Waktu teredit: 31 Maret 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerOfferManagement`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSMarketplaceChangeSetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceOfferManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Offer/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceCreateOfferOnProduct",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : "CreateOfferOnProduct"
        }
      }
    },
    {
```

```
      "Sid" : "AWSMarketplaceListEntities",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceEntitiesReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Offer/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ContainerProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProfessionalServicesProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/SaaSProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/AmiProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ResaleAuthorization/*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceAgreementsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:DescribeAgreement",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        },
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "AWSMarketplaceAgreementsCancellationAndAdjustmentReadAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListAgreementInvoiceLineItems",
        "aws-marketplace:ListBillingAdjustmentRequests",
        "aws-marketplace:GetBillingAdjustmentRequest",
        "aws-marketplace:ListAgreementCancellationRequests",
        "aws-marketplace:GetAgreementCancellationRequest"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        },
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMarketplaceSellerProductsFullAccess

Deskripsi: Menyediakan penjual akses penuh ke halaman Produk AWS Marketplace Manajemen dan AWS layanan lain seperti manajemen AMI.

`AWSMarketplaceSellerProductsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceSellerProductsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Juli 2019, 21:06 UTC
- Waktu teredit: 19 Februari 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MarketplaceListAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:ListEntities",
        "aws-marketplace:ListAssessments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet",
```

```
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*"
    },
    {
      "Sid" : "MarketplaceAssessmentAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeAssessment"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:ModifyImageAttribute",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetIAMRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "IAMPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "assets.marketplace.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "VendorInsightsAccess",
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*"
    },
    {
      "Sid" : "ResourceSharingAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*"
    },
    {
      "Sid" : "MarketplaceEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-files/
${aws:PrincipalAccount}/*"
```

```
      ]
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" :
 "TechnicalStaff"
        }
      }
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMarketplaceSellerProductsReadOnly

Deskripsi: Menyediakan akses baca-saja kepada penjual ke halaman Produk AWS Marketplace Manajemen.

`AWSMarketplaceSellerProductsReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceSellerProductsReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Juli 2019, 21:40 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
```

```
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListAssessments",
        "aws-marketplace:DescribeAssessment",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMcpServiceActionsFullAccess

Deskripsi: Menyediakan akses penuh ke semua tindakan layanan MCP. Kebijakan ini tidak memberikan akses ke tindakan yang diambil oleh MCP, hanya tindakan MCP itu sendiri.

`AWSMcpServiceActionsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMcpServiceActionsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 November 2025, 22:49 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMcpServiceActionsFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllMCPServiceActions",
      "Effect" : "Allow",
      "Action" : "*",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:IsMcpServiceAction" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMCPSignInOAuthAccessPolicy

Deskripsi: Menyediakan akses untuk mengotentikasi ke server AWS MCP menggunakan OAuth AWS Sign-In

`AWSMCPSignInOAuthAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMCPSignInOAuthAccessPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Juli 2026, 06:57 UTC
- Waktu teredit: 09 Juli 2026, 06:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMCPSignInOAuthAccessPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOAuthForAWSMCP",
      "Effect" : "Allow",
      "Action" : [
        "signin:AuthorizeOAuth2Access",
        "signin:CreateOAuth2Token"
      ],
      "Resource" : "arn:aws:signin:*:*:service-principal/aws-mcp.amazonaws.com"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMediaConnectServicePolicy

Deskripsi: Kebijakan default yang memungkinkan akses ke Layanan AWS dan Sumber daya yang digunakan atau dikelola oleh MediaConnect.

`AWSMediaConnectServicePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 03 April 2023, 22:11 UTC
- Waktu teredit: 29 Oktober 2025, 21:34 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:DeleteService",
        "ecs:CreateService",
        "ecs:DescribeServices",
        "ecs:PutAttributes",
        "ecs:DeleteAttributes",
        "ecs:RunTask",
        "ecs:ListTasks",
        "ecs:StartTask",
        "ecs:StopTask",
        "ecs:DescribeTasks",
        "ecs:DescribeContainerInstances",
        "ecs:UpdateContainerInstancesState"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/MediaConnectGateway"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateCluster",
        "ecs:UpdateClusterSettings",
        "ecs:ListAttributes",
        "ecs:DescribeClusters",
        "ecs:DeregisterContainerInstance",
        "ecs:ListContainerInstances"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/MediaConnectGateway"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/created-for-service" : "MediaConnect"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMediaLiveAnywhereServiceRolePolicy

Deskripsi: Mem MediaLive ungkinkan Anywhere untuk membuat dan mengelola AWS sumber daya atas nama Anda.

`AWSMediaLiveAnywhereServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 14 April 2025, 22:07 UTC
- Waktu teredit: 14 April 2025, 22:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaLiveAnywhereServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PutMediaLiveMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/MediaLive"
        }
      }
    },
    {
      "Sid" : "RegisterAnywhereAgentTaskDefinition",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task-definition/MediaLiveAnywhereAgent*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/created_by" : "MediaLiveAnywhere"
        }
      }
    },
    {
      "Sid" : "ECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task-definition/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : "RegisterTaskDefinition",
          "aws:RequestTag/created_by" : "MediaLiveAnywhere"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "created_by"
```

```
        }
      }
    },
    {
      "Sid" : "UpdateAnywhereAgentService",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ecs:Cluster" : "arn:aws:ecs:*:*:cluster/MediaLiveAnywhere*",
          "ecs:Task-Definition" : "arn:aws:ecs:*:*:task-definition/
MediaLiveAnywhereAgent*"
        }
      }
    },
    {
      "Sid" : "ECSListTaskDefinitions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListTaskDefinitions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeregisterAnywhereAgentTaskDefinitionOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeregisterTaskDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeleteAnywhereAgentTaskDefinitionsOnCleanup",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ecs:DeleteTaskDefinitions"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task-definition/MediaLiveAnywhereAgent*"
      ]
    },
    {
      "Sid" : "DeleteAnywhereAgentServiceOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteService"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:service/MediaLiveAnywhere*/MediaLiveAnywhereAgent*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ecs:Cluster" : "arn:aws:ecs:*:*:cluster/MediaLiveAnywhere*"
        }
      }
    },
    {
      "Sid" : "DeregisterContainerInstanceOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListContainerInstances",
        "ecs:DeregisterContainerInstance"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/MediaLiveAnywhere*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMediaTailorServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Sumber AWS daya yang digunakan atau dikelola oleh MediaTailor

`AWSMediaTailorServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 17 September 2021, 22:27 UTC
- Waktu teredit: 17 September 2021, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:MediaTailor/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:MediaTailor/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMigrationHubDiscoveryAccess

Deskripsi: Kebijakan memungkinkan AWSMigrationHubService untuk menelep AWSApplicationDiscoveryService on atas nama pelanggan.

`AWSMigrationHubDiscoveryAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubDiscoveryAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Agustus 2017, 13:30 UTC
- Waktu teredit: 06 Agustus 2020, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
        "discovery:DescribeConfigurations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "dms:AddTagsToResource",
      "Resource" : [
        "arn:aws:dms:*:*:endpoint:*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMigrationHubDMSAccess

Deskripsi: Kebijakan Layanan Migrasi Database untuk mengambil peran dalam akun pelanggan untuk memanggil Pusat Migrasi

`AWSMigrationHubDMSAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubDMSAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Agustus 2017, 14:00 UTC
- Waktu teredit: 07 Oktober 2019, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:CreateProgressUpdateStream"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS"
    },
    {
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:DescribeMigrationTask",
        "mgh:DisassociateCreatedArtifact",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:AssociateDiscoveredResource",
        "mgh:DisassociateDiscoveredResource",
        "mgh:ListDiscoveredResources"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS/*"
    },
    {
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:GetHomeRegion"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMigrationHubFullAccess

Deskripsi: Kebijakan terkelola untuk menyediakan akses pelanggan ke Layanan Migrasi Hub

`AWSMigrationHubFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Agustus 2017, 14:02 UTC
- Waktu teredit: 19 Juni 2019, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:*",
        "discovery:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "continuousexport.discovery.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "migrationhub.amazonaws.com",
            "dmsintegration.migrationhub.amazonaws.com",
            "smsintegration.migrationhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMigrationHubOrchestratorConsoleFullAccess

Deskripsi: Menyediakan akses terbatas ke AWS Migrasi Hub, Layanan Penemuan AWS Aplikasi, Layanan Penyimpanan Sederhana Amazon, dan Manajer AWS Rahasia. Kebijakan ini juga memberikan akses penuh ke layanan AWS Migration Hub Orchestrator.

`AWSMigrationHubOrchestratorConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubOrchestratorConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 20 April 2022, 02:26 UTC
- Waktu teredit: 05 Desember 2023, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MHO",
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-orchestrator:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListAllMyBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "S3MHO",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:ListBucket",
```

```
        "s3:ListBucketVersions",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::migrationhub-orchestrator-*",
        "arn:aws:s3:::migrationhub-orchestrator-*/*"
      ]
    },
    {
      "Sid" : "ListSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Configuration",
      "Effect" : "Allow",
      "Action" : [
        "discovery:DescribeConfigurations",
        "discovery:ListConfigurations",
        "discovery:GetDiscoverySummary"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetHomeRegion",
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "KMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMListProfileRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Account",
      "Effect" : "Allow",
      "Action" : [
        "account:ListRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "migrationhub-orchestrator.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "GetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/migrationhub-
orchestrator.amazonaws.com/AWSServiceRoleForMigrationHubOrchestrator*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMigrationHubOrchestratorInstanceRolePolicy

Deskripsi: Kebijakan ini perlu dilampirkan untuk instans yang dimigrasi SAP dan MGN untuk layanan kami untuk mengatur instans dengan mengunduh skrip dari S3 dan untuk mengambil nilai rahasia di dalam instans EC2.

`AWSMigrationHubOrchestratorInstanceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubOrchestratorInstanceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 April 2022, 02:43 UTC
- Waktu teredit: 20 April 2022, 02:43 UTC

- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorInstanceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-orchestrator-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::migrationhub-orchestrator-*",
        "arn:aws:s3:::aws-migrationhub-orchestrator-*/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMigrationHubOrchestratorPlugin

Deskripsi: Menyediakan akses terbatas ke Layanan Penyimpanan Sederhana Amazon, Manajer AWS Rahasia, dan tindakan terkait Plugin untuk AWS Migration Hub Orchestrator.

`AWSMigrationHubOrchestratorPlugin`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubOrchestratorPlugin` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 April 2022, 02:25 UTC
- Waktu teredit: 20 April 2022, 02:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetBucketAcl"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-orchestrator-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "execute-api:ManageConnections"
      ],
      "Resource" : [
        "arn:aws:execute-api:*:*:*/prod/*/put-log-data",
        "arn:aws:execute-api:*:*:*/prod/*/put-metric-data"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-orchestrator:RegisterPlugin",
        "migrationhub-orchestrator:GetMessage",
        "migrationhub-orchestrator:SendMessage"
      ],
      "Resource" : "arn:aws:migrationhub-orchestrator:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-orchestrator-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMigrationHubOrchestratorServiceRolePolicy

Deskripsi: Menyediakan izin yang diperlukan untuk Migration Hub Orchestrator untuk memigrasikan dan memodernisasi beban kerja lokal Anda

`AWSMigrationHubOrchestratorServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 20 April 2022, 02:24 UTC
- Waktu teredit: 04 Maret 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubOrchestratorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationDiscoveryService",
      "Effect" : "Allow",
      "Action" : [
        "discovery:DescribeConfigurations",
        "discovery:ListConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LaunchWizard",
      "Effect" : "Allow",
      "Action" : [
        "launchwizard:ListProvisionedApps",
        "launchwizard:DescribeProvisionedApp",
        "launchwizard:ListDeployments",
        "launchwizard:GetDeployment"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2instances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ec2MGNLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "mgn.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ec2LaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeLaunchTemplates"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "getHomeRegion",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMcommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetCommandInvocation",
        "ssm:CancelCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunRemoteScript",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:s3:::aws-migrationhub-orchestrator-*",
        "arn:aws:s3:::migrationhub-orchestrator-*"
      ]
    },
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "s3GetObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::migrationhub-orchestrator-*",
        "arn:aws:s3:::migrationhub-orchestrator-*/*"
      ]
    },
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:DeleteRule",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/MigrationHubOrchestratorManagedRule*"
    },
    {
      "Sid" : "MGN",
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetReplicationConfiguration",
        "mgn:GetLaunchConfiguration",
        "mgn:StartCutover",
        "mgn:FinalizeCutover",
        "mgn:StartTest",
        "mgn:UpdateReplicationConfiguration",
        "mgn:DescribeSourceServers",
        "mgn:MarkAsArchived",
        "mgn:ChangeServerLifeCycleState"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ec2DescribeImportImage",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeImportImageTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "s3ListBucket",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : "migrationhub-orchestrator-vmie-*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

Deskripsi: Memberikan akses penuh ke AWS Migration Hub Refactor Spaces dan layanan AWS terkait lainnya kecuali AWS grup keamanan Transit Gateway dan EC2 yang tidak diperlukan saat menggunakan lingkungan tanpa jembatan jaringan. Kebijakan ini juga mengecualikan izin yang diperlukan untuk AWS Lambda dan AWS Resource Access Manager karena dapat dicakup berdasarkan tag.

`AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 April 2023, 20:09 UTC
- Waktu teredit: 11 April 2024, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RefactorSpaces",
      "Effect" : "Allow",
      "Action" : [
        "refactor-spaces:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpointServiceConfigurations",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpcEndpointServiceConfigurationCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagsDelete",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Sid" : "VpcEndpointServiceConfigurationDelete",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBLoadBalancerCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
```

```
        "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ELBModify",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
          ]
        }
      }
    },
    {
      "Sid" : "ELBLoadBalancerDelete",
      "Effect" : "Allow",
```

```
      "Action" : "elasticloadbalancing:DeleteLoadBalancer",
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
    },
    {
      "Sid" : "ELBListenerCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBListenerDelete",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteListener",
      "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    },
    {
      "Sid" : "ELBTargetGroupModify",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
    },
    {
      "Sid" : "ELBTargetGroupCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
```

```
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Sid" : "APIGatewayModify",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:DELETE",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:UpdateRestApiPolicy"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*",
        "arn:aws:apigateway:*::/tags",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "APIGatewayVpcLinksGet",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "OrganizationDescribe",
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationStackCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationStackTag",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/*"
    },
    {
      "Sid" : "CreateRefactorSpacesSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateELBSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

Deskripsi: Gunakan peran layanan IAM yang diteruskan ke dokumen Otomasi SSM untuk memberikan izin AWSRefactorSpaces-CreateResources yang diperlukan untuk menjalankan otomatisasi. Kebijakan ini memberikan read/write akses ke tag EC2 untuk melacak kemajuan otomatisasi. Ketika jembatan jaringan lingkungan Refactor Spaces diaktifkan, otomatisasi juga menambahkan grup keamanan lingkungan ke instance EC2 untuk mengizinkan lalu lintas dari layanan Refactor Spaces lainnya di lingkungan. Kebijakan ini juga memberikan akses ke parameter SSM tindakan pasca peluncuran Layanan Migrasi Aplikasi.

`AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubRefactorSpaces-SSMAutomationPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 10 Agustus 2023, 15:08 UTC
- Waktu teredit: 10 Agustus 2023, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/refactor-spaces:ssm:optin" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/refactor-spaces:ssm:optin" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "refactor-spaces:ssm:environment-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:GetParameters",
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMigrationHubRefactorSpacesFullAccess

Deskripsi: Memberikan akses penuh ke AWS MigrationHub Refactor Spaces, fitur konsol AWS MigrationHub Refactor Spaces, dan AWS layanan terkait lainnya kecuali izin yang diperlukan untuk AWS Lambda dan AWS Resource Access Manager karena dapat dicakup berdasarkan tag.

`AWSMigrationHubRefactorSpacesFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubRefactorSpacesFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2021, 07:12 UTC
- Waktu teredit: 11 April 2024, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RefactorSpaces",
      "Effect" : "Allow",
      "Action" : [
        "refactor-spaces:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcs",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RequestTagTransitGatewayCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGateway",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Sid" : "ResourceTagTransitGatewayCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGateway",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Sid" : "VpcEndpointServiceConfigurationCreate",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2NetworkingModify",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTransitGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Sid" : "VpcEndpointServiceConfigurationDelete",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBLoadBalancerCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateLoadBalancer"
      ],
```

```
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ELBModify",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
          ]
        }
      }
    },
    {
      "Sid" : "ELBLoadBalancerDelete",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteLoadBalancer",
```

```
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
    },
    {
      "Sid" : "ELBListenerCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBListenerDelete",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteListener",
      "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    },
    {
      "Sid" : "ELBTargetGroupModify",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
    },
    {
      "Sid" : "ELBTargetGroupCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
```

```
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Sid" : "APIGatewayModify",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:DELETE",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:UpdateRestApiPolicy"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*",
        "arn:aws:apigateway:*::/tags",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "APIGatewayVpcLinksGet",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "OrganizationDescribe",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationStackCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationStackTag",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/*"
    },
    {
      "Sid" : "CreateRefactorSpacesSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateELBSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMigrationHubRefactorSpacesServiceRolePolicy

Deskripsi: Menyediakan akses ke AWS Sumber Daya yang dikelola atau digunakan oleh AWS Migration Hub Refactor Spaces.

`AWSMigrationHubRefactorSpacesServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 29 November 2021, 06:50 UTC
- Waktu teredit: 20 Juli 2023, 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:DeleteTags",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:PUT",
        "apigateway:POST",
        "apigateway:GET",
        "apigateway:PATCH",
        "apigateway:DELETE"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks/*",
        "arn:aws:apigateway:*::/tags",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
```

```
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : "arn:aws:apigateway:*::/vpclinks/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteLoadBalancer",
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteListener",
      "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMigrationHubSMSAccess

Deskripsi: Kebijakan Layanan Migrasi Server untuk mengambil peran dalam akun pelanggan untuk memanggil Migrasi Hub

`AWSMigrationHubSMSAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubSMSAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Agustus 2017, 13:57 UTC
- Waktu teredit: 07 Oktober 2019, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:CreateProgressUpdateStream"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS"
    },
    {
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:DescribeMigrationTask",
        "mgh:DisassociateCreatedArtifact",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes",
```

```
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:AssociateDiscoveredResource",
        "mgh:DisassociateDiscoveredResource",
        "mgh:ListDiscoveredResources"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS/*"
    },
    {
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:GetHomeRegion"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMigrationHubStrategyCollector

Deskripsi: Memberikan izin untuk mengizinkan komunikasi dengan layanan Rekomendasi Strategi Pusat AWS Migrasi, read/write akses ke bucket S3 yang terkait dengan layanan, akses Amazon API Gateway untuk mengunggah log dan metrik AWS, akses Manajer AWS Rahasia untuk mengambil kredentif, dan layanan terkait apa pun.

`AWSMigrationHubStrategyCollector`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubStrategyCollector` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Oktober 2021, 20:15 UTC
- Waktu teredit: 01 April 2024, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MHSRAllowS3Resources",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration",
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "MHSRAllowS3ListBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MHSRAllowMetricsAndLogs",
      "Effect" : "Allow",
      "Action" : [
        "application-transformation:PutMetricData",
        "application-transformation:PutLogData",
        "application-transformation:StartPortingCompatibilityAssessment",
        "application-transformation:GetPortingCompatibilityAssessment",
        "application-transformation:StartPortingRecommendationAssessment",
        "application-transformation:GetPortingRecommendationAssessment"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MHSRAllowExecuteAPI",
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "execute-api:ManageConnections"
      ],
      "Resource" : [
        "arn:aws:execute-api:*:*:*/prod/*/put-log-data",
        "arn:aws:execute-api:*:*:*/prod/*/put-metric-data"
      ]
    },
    {
      "Sid" : "MHSRAllowCollectorAPI",
      "Effect" : "Allow",
      "Action" : [
```

```
        "migrationhub-strategy:RegisterCollector",
        "migrationhub-strategy:GetAntiPattern",
        "migrationhub-strategy:GetMessage",
        "migrationhub-strategy:SendMessage",
        "migrationhub-strategy:ListAntiPatterns",
        "migrationhub-strategy:ListJarArtifacts",
        "migrationhub-strategy:UpdateCollectorConfiguration",
        "migrationhub-strategy:PutLogData",
        "migrationhub-strategy:PutMetricData"
      ],
      "Resource" : "arn:aws:migrationhub-strategy:*:*:*"
    },
    {
      "Sid" : "MHSRAllowSecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-strategy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMigrationHubStrategyConsoleFullAccess

Deskripsi: Memberikan akses penuh ke layanan Rekomendasi Strategi Pusat AWS Migrasi dan akses ke AWS layanan terkait melalui Konsol Manajemen AWS.

`AWSMigrationHubStrategyConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubStrategyConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Oktober 2021, 20:13 UTC
- Waktu teredit: 09 November 2022, 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-strategy:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "discovery:GetDiscoverySummary",
        "discovery:DescribeTags",
        "discovery:DescribeConfigurations",
        "discovery:ListConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "migrationhub-strategy.amazonaws.com"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/migrationhub-
strategy.amazonaws.com/AWSMigrationHubStrategyServiceRolePolicy*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMigrationHubStrategyServiceRolePolicy

Deskripsi: Aktifkan akses ke AWS Sumber Daya yang digunakan atau dikelola oleh layanan Rekomendasi Strategi Pusat AWS Migrasi.

`AWSMigrationHubStrategyServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 19 Oktober 2021, 20:02 UTC
- Waktu teredit: 19 Oktober 2021, 20:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubStrategyServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "permissionsForAds",
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
        "discovery:DescribeConfigurations",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "permissionsForS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMobileHub_FullAccess

Deskripsi: Kebijakan ini dapat dilampirkan ke Pengguna, Peran, atau Grup mana pun, untuk memberikan izin kepada pengguna untuk membuat, menghapus, dan memodifikasi proyek (dan AWS sumber daya terkaitnya) di AWS Mobile Hub. Ini juga termasuk izin untuk menghasilkan dan mengunduh contoh kode sumber aplikasi seluler untuk setiap proyek Mobile Hub.

`AWSMobileHub_FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMobileHub_FullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Januari 2016, 19:56 UTC
- Waktu teredit: 19 Desember 2019, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_FullAccess`

Versi kebijakan

Versi kebijakan: v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:POST",
        "cloudfront:GetDistribution",
        "devicefarm:CreateProject",
        "devicefarm:ListJobs",
        "devicefarm:ListRuns",
        "devicefarm:GetProject",
        "devicefarm:GetRun",
        "devicefarm:ListArtifacts",
        "devicefarm:ListProjects",
        "devicefarm:ScheduleRun",
        "dynamodb:DescribeTable",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "iam:ListSAMLProviders",
        "lambda:ListFunctions",
        "sns:ListTopics",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetBot",
        "lex:GetBots",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "mobilehub:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
```

```
      "Resource" : "arn:aws:s3:::*/aws-my-sample-app*.zip"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*-mobilehub-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*-mobilehub-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMobileHub_ReadOnly

Deskripsi: Kebijakan ini dapat dilampirkan ke Pengguna, Peran, atau Grup mana pun, untuk memberikan izin kepada pengguna untuk membuat daftar dan melihat proyek di AWS Mobile Hub. Ini juga termasuk izin untuk menghasilkan dan mengunduh contoh kode sumber aplikasi seluler untuk setiap proyek Mobile Hub. Itu tidak memungkinkan pengguna untuk memodifikasi konfigurasi apa pun untuk proyek Mobile Hub apa pun.

`AWSMobileHub_ReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMobileHub_ReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Januari 2016, 19:55 UTC
- Waktu teredit: 23 Juli 2018, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_ReadOnly`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "iam:ListSAMLProviders",
        "lambda:ListFunctions",
        "sns:ListTopics",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetBot",
        "lex:GetBots",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "mobilehub:ExportProject",
        "mobilehub:GenerateProjectParameters",
        "mobilehub:GetProject",
        "mobilehub:SynchronizeProject",
        "mobilehub:GetProjectSnapshot",
```

```
        "mobilehub:ListProjectSnapshots",
        "mobilehub:ListAvailableConnectors",
        "mobilehub:ListAvailableFeatures",
        "mobilehub:ListAvailableRegions",
        "mobilehub:ListProjects",
        "mobilehub:ValidateProject",
        "mobilehub:VerifyServiceRole",
        "mobilehub:DescribeBundle",
        "mobilehub:ExportBundle",
        "mobilehub:ListBundles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/aws-my-sample-app*.zip"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSMSKReplicatorExecutionRole

Deskripsi: Memberikan izin kepada Amazon MSK Replicator untuk mereplikasi data antar Cluster MSK.

`AWSMSKReplicatorExecutionRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMSKReplicatorExecutionRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Desember 2023, 00:07 UTC
- Waktu teredit: 25 Maret 2024, 21:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:Connect",
        "kafka-cluster:DescribeCluster",
        "kafka-cluster:AlterCluster",
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:CreateTopic",
        "kafka-cluster:AlterTopic",
        "kafka-cluster:WriteData",
        "kafka-cluster:ReadData",
        "kafka-cluster:AlterGroup",
        "kafka-cluster:DescribeGroup",
```

```
        "kafka-cluster:DescribeTopicDynamicConfiguration",
        "kafka-cluster:AlterTopicDynamicConfiguration",
        "kafka-cluster:WriteDataIdempotently"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "TopicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:CreateTopic",
        "kafka-cluster:AlterTopic",
        "kafka-cluster:WriteData",
        "kafka-cluster:ReadData",
        "kafka-cluster:DescribeTopicDynamicConfiguration",
        "kafka-cluster:AlterTopicDynamicConfiguration",
        "kafka-cluster:AlterCluster"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:topic/*/*"
      ]
    },
    {
      "Sid" : "GroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:AlterGroup",
        "kafka-cluster:DescribeGroup"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:group/*/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSNATGatewayServiceRolePolicy

Deskripsi: Memberikan izin untuk mengelola sumber daya VPC untuk konfigurasi dan pengelolaan NAT Gateway.

`AWSNATGatewayServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 14 November 2025, 17:19 UTC
- Waktu teredit: 14 November 2025, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNATGatewayServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSNetworkFirewallFullAccess

Deskripsi: Memberikan akses penuh ke layanan Firewall AWS Jaringan, termasuk izin untuk membuat, mengonfigurasi, mengelola, dan menghapus sumber daya firewall, kebijakan, dan grup aturan. Selain itu termasuk izin untuk memodifikasi titik akhir VPC, kebijakan bucket S3, konfigurasi CloudWatch Log, dan membuat peran terkait layanan untuk Firewall Jaringan dan layanan pengiriman log

`AWSNetworkFirewallFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSNetworkFirewallFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 Juni 2025, 21:52 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkFirewallFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NetworkFirewall",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:ListAnalysisReports",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListFlowOperations",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListTLSInspectionConfigurations",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeFlowOperation",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:GetAnalysisReportResults",
        "network-firewall:ListFlowOperationResults",
        "network-firewall:TagResource",
        "network-firewall:UntagResource",
        "network-firewall:AssociateFirewallPolicy",
        "network-firewall:AssociateSubnets",
        "network-firewall:CreateFirewall",
        "network-firewall:CreateFirewallPolicy",
        "network-firewall:CreateRuleGroup",
        "network-firewall:CreateTLSInspectionConfiguration",
        "network-firewall:DeleteFirewall",
```

```
        "network-firewall:DeleteFirewallPolicy",
        "network-firewall:DeleteResourcePolicy",
        "network-firewall:DeleteRuleGroup",
        "network-firewall:DeleteTLSInspectionConfiguration",
        "network-firewall:DisassociateSubnets",
        "network-firewall:PutResourcePolicy",
        "network-firewall:StartAnalysisReport",
        "network-firewall:StartFlowCapture",
        "network-firewall:StartFlowFlush",
        "network-firewall:UpdateFirewallAnalysisSettings",
        "network-firewall:UpdateFirewallDeleteProtection",
        "network-firewall:UpdateFirewallDescription",
        "network-firewall:UpdateFirewallEncryptionConfiguration",
        "network-firewall:UpdateFirewallPolicy",
        "network-firewall:UpdateFirewallPolicyChangeProtection",
        "network-firewall:UpdateLoggingConfiguration",
        "network-firewall:UpdateRuleGroup",
        "network-firewall:UpdateSubnetChangeProtection",
        "network-firewall:UpdateTLSInspectionConfiguration"
      ],
      "Resource" : [
        "arn:aws:network-firewall:*:*:*"
      ]
    },
    {
      "Sid" : "NetworkFirewallEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallCreateVpcEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkFirewallDeleteVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkFirewallLogging",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallLoggingCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Sid" : "NetworkFirewallLoggingS3",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "NetworkFirewallLoggingFirehose",
      "Effect" : "Allow",
      "Action" : "firehose:TagDeliveryStream",
      "Resource" : "arn:aws:firehose:*:*:*"
    },
    {
      "Sid" : "NetworkFirewallSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/network-firewall.amazonaws.com/
AWSServiceRoleForNetworkFirewall"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "network-firewall.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "NetworkFirewallLogDeliverySLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSNetworkFirewallReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke sumber daya AWS Network Firewall melalui Konsol Manajemen AWS, CLI, dan SDK. Kebijakan ini memungkinkan pengguna untuk melihat dan memantau konfigurasi firewall, kebijakan, grup aturan, dan sumber daya terkait, tanpa kemampuan untuk membuat perubahan.

`AWSNetworkFirewallReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSNetworkFirewallReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 Juni 2025, 21:52 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkFirewallReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:ListAnalysisReports",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListFlowOperations",
        "network-firewall:ListProxies",
        "network-firewall:ListProxyConfigurations",
        "network-firewall:ListProxyRuleGroups",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListTLSInspectionConfigurations",
        "network-firewall:ListVpcEndpointAssociations",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallMetadata",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeFlowOperation",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeProxy",
        "network-firewall:DescribeProxyConfiguration",
        "network-firewall:DescribeProxyRule",
        "network-firewall:DescribeProxyRuleGroup",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:DescribeVpcEndpointAssociation",
        "network-firewall:GetAnalysisReportResults",
        "network-firewall:ListFlowOperationResults"
      ],
      "Resource" : "arn:aws:network-firewall:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries"
```

```
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSNetworkFirewallServiceRolePolicy

Deskripsi: Izinkan AWSNetworkFirewall untuk membuat dan mengelola sumber daya yang diperlukan untuk Firewall Anda.

`AWSNetworkFirewallServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 17 November 2020, 17:17 UTC
- Waktu teredit: 01 Juni 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkFirewallServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "acm:DescribeCertificate",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroupResources",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "resource-groups.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListContainerInstances",
        "ecs:ListTasks",
        "ecs:DescribeTasks",
        "ecs:DescribeContainerInstances"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/*",
        "arn:aws:ecs:*:*:container-instance/*/*",
        "arn:aws:ecs:*:*:task/*/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSNetworkManagerCloudWANServiceRolePolicy

Deskripsi: Izinkan NetworkManager untuk mengakses sumber daya yang terkait dengan Jaringan Inti Anda

`AWSNetworkManagerCloudWANServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 12 Juli 2022, 12:17 UTC
- Waktu teredit: 12 Juli 2022, 12:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
```

```
        "ec2:DeleteTransitGatewayRouteTableAnnouncement",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:DisableTransitGatewayRouteTablePropagation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSNetworkManagerFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon NetworkManager melalui Konsol Manajemen AWS.

`AWSNetworkManagerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSNetworkManagerFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 17:37 UTC
- Waktu teredit: 03 Desember 2019, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "networkmanager:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "networkmanager.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSNetworkManagerReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon NetworkManager melalui Konsol Manajemen AWS.

`AWSNetworkManagerReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSNetworkManagerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2019, 17:35 UTC
- Waktu teredit: 03 Desember 2019, 17:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:Describe*",
        "networkmanager:Get*",
        "networkmanager:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSNetworkManagerServiceRolePolicy

Deskripsi: Izinkan NetworkManager untuk mengakses sumber daya yang terkait dengan Jaringan Global Anda

`AWSNetworkManagerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 03 Desember 2019, 14:03 UTC
- Waktu teredit: 27 Juli 2022 19.41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeLocations",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpcs",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeRegions",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "ec2:DescribeTransitGatewayRouteTableAnnouncements",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:GetTransitGatewayPolicyTableAssociations",
        "ec2:GetTransitGatewayPolicyTableEntries"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSObservabilityAdminLogsCentralizationServiceRolePolicy

Deskripsi: izin Service-linked peran untuk sentr CloudWatch alisasi Log

`AWSObservabilityAdminLogsCentralizationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 15 September 2025, 14:34 UTC
- Waktu teredit: 15 September 2025, 14:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminLogsCentralizationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "logs.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/LogsManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:logs:arn" : "arn:aws:logs:*:*:log-group:*"
        }
      },
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSObservabilityAdminServiceRolePolicy

Deskripsi: Menyediakan akses untuk mengelola AWS Perekam Konfigurasi AWS Konfigurasi, mengelola Agregator Konfigurasi Konfigurasi, membuat Peran Tertaut Layanan Kon AWS fig untuk fungsionalitas Perekam Konfigurasi, menggunakan data konfigurasi perekam, dan membaca AWS data Organisasi untuk fitur organisasi.

`AWSObservabilityAdminServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 27 November 2024, 19:36 UTC
- Waktu teredit: 14 Juli 2026, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
```

```
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder"
      ],
      "Resource" : [
        "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForObservabilityAdmin/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigurationAggregator",
        "config:DeleteConfigurationAggregator",
        "config:SelectAggregateResourceConfig"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
observabilityadmin.amazonaws.com/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
```

```
            "config.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "config.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "config.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "organizations:ServicePrincipal" : [
            "observabilityadmin.amazonaws.com",
            "config.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSObservabilityAdminTelemetryEnablementServiceRolePolicy

Deskripsi: Menyediakan akses untuk mengelola sumber daya perekam AWS konfigurasi dan pengaturan telemetri pada AWS sumber daya termasuk log, metrik.

`AWSObservabilityAdminTelemetryEnablementServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 01 Agustus 2025, 18:04 UTC
- Waktu teredit: 23 September 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminTelemetryEnablementServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TelemetryOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeFlowLogs",
        "ec2:DescribeVpcs",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "logs:ListLogGroups",
        "ec2:MonitorInstances",
        "logs:DescribeDeliverySources",
        "logs:DescribeDeliveries",
        "logs:DescribeDeliveryDestinations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagOperationForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : "CloudWatchTelemetryRuleManaged"
        },
        "StringEquals" : {
          "aws:RequestTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ec2:CreateAction" : "CreateFlowLogs"
        }
      }
    },
    {
      "Sid" : "TagOperationForLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchTelemetryRuleManaged"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForVPCLogs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFlowLogs"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForVPCFlowLogs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFlowLogs"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-flow-log/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchTelemetryRuleManaged"
        },
        "StringEquals" : {
          "aws:RequestTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForLogs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteFlowLogs",
        "logs:CreateDelivery",
        "logs:CreateLogGroup",
        "logs:PutResourcePolicy",
        "logs:PutRetentionPolicy",
        "logs:PutDeliveryDestination",
        "logs:PutDeliverySource",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSApiLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "Bool" : {
          "eks:loggingType/api" : "true"
```

```
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSAuditLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "Bool" : {
          "eks:loggingType/audit" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSAuthenticatorLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "Bool" : {
          "eks:loggingType/authenticator" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSControllerManagerLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
```

```
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "Bool" : {
          "eks:loggingType/controllerManager" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSSchedulerLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "Bool" : {
          "eks:loggingType/scheduler" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForWafLoggingConfigurations",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration"
      ],
      "Resource" : "arn:aws:wafv2:*:*:*/webacl/*",
      "Condition" : {
        "ArnLike" : {
          "wafv2:LogDestinationResource" : "arn:aws:logs:*:*:log-group:*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "wafv2:LogScope" : "CloudwatchTelemetryRuleManaged"
        }
      }
    },
    {
```

```
      "Sid" : "TelemetryReadForWafLoggingConfigurations",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:ListLoggingConfigurations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForWafLogDelivery",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AllowVendedLogDeliveryForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "TelemetryOperationsForBedrock",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:AllowVendedLogDeliveryForResource",
        "bedrock:AllowVendedLogDeliveryForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:AllowVendedLogDeliveryForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForSecurityHub",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:AllowVendedLogDeliveryForResource",
        "securityhub:DescribeHub",
        "securityhub:DescribeSecurityHubV2"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForCloudfront",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudfront:AllowVendedLogDeliveryForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForCloudTrailLogs",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:UpdateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/cloudwatch/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForManagedLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutResourcePolicy",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws/cloudtrail",
        "arn:aws:logs:*:*:log-group:aws/cloudtrail/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "Route53QueryLoggingListOperations",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverQueryLogConfigAssociations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Route53QueryLoggingGetOperations",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Route53QueryLoggingConfigCreation",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:CreateResolverQueryLogConfig",
        "route53resolver:TagResource"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:resolver-query-log-config/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "Route53QueryLoggingConfigAssociation",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:AssociateResolverQueryLogConfig"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForRoute53LogDeliverySLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:*:iam::*:role/aws-service-role/route53resolver.amazonaws.com/
AWSServiceRoleForRoute53Resolver",
      "Condition" : {
        "BoolIfExists" : {
          "aws:ViaAWSService" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:AWSServiceName" : [
            "route53resolver.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForRoute53LogDelivery",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMOperationsForConfigServiceLinkedRecorder",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "BoolIfExists" : {
          "aws:ViaAWSService" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:AWSServiceName" : [
            "config.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManagementOperationsForServiceLinkedRecorder",
      "Effect" : "Allow",
      "Action" : [
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:AssociateResourceTypes",
        "config:DisassociateResourceTypes"
      ],
      "Resource" : [
        "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForObservabilityAdmin_TelemetryEnablement/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReadOperationsForServiceLinkedRecorder",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders"
      ],
```

```
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "config:ConfigurationRecorderServicePrincipal" : [
            "telemetry-enablement.observabilityadmin.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForKafka",
      "Effect" : "Allow",
      "Action" : [
        "kafka:UpdateMonitoring",
        "kafka:DescribeCluster"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForOTelEnrichmentSimba",
      "Effect" : "Allow",
      "Action" : [
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:StartTelemetryEnrichment",
        "observabilityadmin:StopTelemetryEnrichment"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForOTelEnrichmentResourceExplorer",
      "Effect" : "Allow",
```

```
      "Action" : [
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:CreateManagedView",
        "resource-explorer-2:CreateStreamingAccessForService",
        "resource-explorer-2:DeleteStreamingAccessForService"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForOTelEnrichmentCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetOTelEnrichment",
        "cloudwatch:StartOTelEnrichment"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForOTelEnrichmentSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "StringEquals" : {
          "iam:AWSServiceName" : "resource-explorer-2.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "TelemetryReadTagsForLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryKMSOperationsForAccount",
      "Effect" : "Allow",
      "Action" : [
        "kms:Describe*",
        "logs:AssociateKmsKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryKMSOperationsForOrganization",
      "Effect" : "Allow",
      "Action" : [
        "kms:Describe*",
        "logs:AssociateKmsKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalOrgId" : "${aws:ResourceOrgId}"
        }
      }
```

```
    },
    {
      "Sid" : "InspectTemplate",
      "Effect" : "Allow",
      "Action" : "iam:GetRoleTemplateVersion",
      "Resource" : "arn:aws:iam::aws:role-template/telemetry-
enablement.observabilityadmin.amazonaws.com/
CloudWatchTelemetryRuleEKSAddonRoleTemplate:1"
    },
    {
      "Sid" : "AcquireRoleFromTemplate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/
CloudWatchTelemetryRuleEKSAddonRole",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:RoleTemplateARN" : "arn:aws:iam::aws:role-
template/telemetry-enablement.observabilityadmin.amazonaws.com/
CloudWatchTelemetryRuleEKSAddonRoleTemplate:1"
        }
      }
    },
    {
      "Sid" : "AttachManagedPolicyFromTemplate",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Resource" : "arn:aws:iam::*:role/service-role/
CloudWatchTelemetryRuleEKSAddonRole",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:RoleTemplateARN" : "arn:aws:iam::aws:role-
template/telemetry-enablement.observabilityadmin.amazonaws.com/
CloudWatchTelemetryRuleEKSAddonRoleTemplate:1"
        }
      }
```

```
    },
    {
      "Sid" : "ReadRole",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchTelemetryRuleEKSAddonRole",
        "arn:aws:iam::*:role/CloudWatchTelemetryRuleEKSAddonRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PassRoleToPodIdentity",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
CloudWatchTelemetryRuleEKSAddonRole",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : "pods.eks.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InstallAddon",
      "Effect" : "Allow",
      "Action" : "eks:CreateAddon",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "FixAddon",
      "Effect" : "Allow",
      "Action" : "eks:UpdateAddon",
      "Resource" : "arn:aws:eks:*:*:addon/*/amazon-cloudwatch-observability/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CreatePodIdentityAssociation",
      "Effect" : "Allow",
      "Action" : "eks:CreatePodIdentityAssociation",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "FixPodIdentityAssociation",
      "Effect" : "Allow",
      "Action" : "eks:UpdatePodIdentityAssociation",
      "Resource" : "arn:aws:eks:*:*:podidentityassociation/*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EvaluateAddon",
      "Effect" : "Allow",
      "Action" : "eks:DescribeAddon",
      "Resource" : "arn:aws:eks:*:*:addon/*/amazon-cloudwatch-observability/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListPodIdentityAssociations",
      "Effect" : "Allow",
      "Action" : "eks:ListPodIdentityAssociations",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EvaluatePodIdentityAssociation",
      "Effect" : "Allow",
      "Action" : "eks:DescribePodIdentityAssociation",
      "Resource" : "arn:aws:eks:*:*:podidentityassociation/*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSOrganizationsFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Organisasi.

`AWSOrganizationsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSOrganizationsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 November 2018, 20:31 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC

- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsFullAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSOrganizationsFullAccess",
      "Effect" : "Allow",
      "Action" : "organizations:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:PutAlternateContact",
        "account:DeleteAlternateContact",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:PutContactInformation",
        "account:ListRegions",
        "account:EnableRegion",
        "account:DisableRegion",
        "account:PutAccountName",
        "account:GetAccountInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "organizations.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSOrganizationsReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke AWS Organisasi.

`AWSOrganizationsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSOrganizationsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 November 2018, 20:32 UTC
- Waktu teredit: 07 Juni 2024, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSOrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsReadOnlyAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:ListRegions",
        "account:GetRegionOptStatus",
        "account:GetPrimaryEmail"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSOrganizationsServiceTrustPolicy

Deskripsi: Kebijakan untuk mengiz AWS inkan Organisasi berbagi kepercayaan dengan pihak lain yang disetujui Layanan AWS untuk tujuan menyederhanakan konfigurasi pelanggan.

`AWSOrganizationsServiceTrustPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 10 Oktober 2017, 23:04 UTC
- Waktu teredit: 05 Maret 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOrganizationsServiceTrustPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDeletionOfServiceLinkedRoleForOrganizations",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/organizations.amazonaws.com/*"
      ]
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListRolesSLR",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSOutpostsAuthorizeServerPolicy

Deskripsi: Kebijakan ini memberikan izin yang memungkinkan Anda menginstal server Outpost di jaringan lokal Anda.

`AWSOutpostsAuthorizeServerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSOutpostsAuthorizeServerPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 04 Januari 2023, 19:23 UTC
- Waktu teredit: 04 Januari 2023, 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:StartConnection",
        "outposts:GetConnection"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSOutpostsServiceRolePolicy

Deskripsi: Kebijakan Peran Tertaut Layanan untuk mengaktifkan akses ke AWS sumber daya yang dikelola oleh Pos Ter AWS depan

`AWSOutpostsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 09 November 2020, 22:55 UTC
- Waktu teredit: 17 April 2025, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOutpostsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrivateConnectivityServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateConnectivityCreateNetworkInterfacePolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc/*",
        "arn:*:ec2:*:*:subnet/*",
        "arn:*:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "PrivateConnectivityCreateNetworkInterfaceTaggingPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "outposts:private-connectivity-resourceId"
          ]
        }
      }
    },
    {
      "Sid" : "PrivateConnectivityCreateSecurityGroupPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc/*"
      ]
    },
    {
```

```
      "Sid" : "PrivateConnectivityCreateSecurityGroupTaggingPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "outposts:private-connectivity-resourceId"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPanoramaApplianceRolePolicy

Deskripsi: Mengizinkan perangkat lunak AWS IoT pada AWS Panorama Appliance untuk mengunggah log ke Amazon CloudWatch.

`AWSPanoramaApplianceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPanoramaApplianceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Desember 2020, 13:13 UTC

- Waktu teredit: 01 Desember 2020, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaDeviceCreateLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*"
    },
    {
      "Sid" : "PanoramaDeviceCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/panorama_device*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPanoramaApplianceServiceRolePolicy

Deskripsi: Mengiz AWS inkan Panorama Appliance mengunggah log ke Amazon CloudWatch, dan mendapatkan objek dari titik akses Amazon S3 yang dibuat untuk digunakan dengan AWS Panorama.

`AWSPanoramaApplianceServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPanoramaApplianceServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 Oktober 2021, 12:14 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaDeviceCreateLogStream",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Sid" : "PanoramaDeviceCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Sid" : "PanoramaDevicePutMetric",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "PanoramaDeviceMetrics"
        }
      }
    },
    {
      "Sid" : "PanoramaDeviceS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetObjectVersion"
      ],
      "Resource" : [
        "arn:aws:s3:::*-nodepackage-store-*",
        "arn:aws:s3:::*-application-payload-store-*",
        "arn:aws:s3:*:*:accesspoint/panorama*"
      ],
```

```
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPanoramaFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Panorama

`AWSPanoramaFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPanoramaFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2020, 13:12 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPanoramaFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "panorama:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:panorama*",
```

```
        "arn:aws:secretsmanager:*:*:secret:Panorama*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "panorama.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
```

```
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "panorama.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPanoramaGreengrassGroupRolePolicy

Deskripsi: Mengizinkan fungsi AWS Lambda pada AWS Panorama Appliance untuk mengelola sumber daya di Panorama, mengunggah log dan metrik ke Amazon CloudWatch, dan mengelola objek dalam bucket yang dibuat untuk digunakan dengan Panorama.

`AWSPanoramaGreengrassGroupRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPanoramaGreengrassGroupRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Desember 2020, 13:10 UTC
- Waktu teredit: 06 Januari 2021 19.30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucket*",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
```

```
    },
    {
      "Sid" : "PanoramaCLoudWatchPutDashboard",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutDashboard",
      "Resource" : [
        "arn:aws:cloudwatch::*:dashboard/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaCloudWatchPutMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "PanoramaGreenGrassCloudWatchAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/greengrass/*"
    },
    {
      "Sid" : "PanoramaAccess",
      "Effect" : "Allow",
      "Action" : [
        "panorama:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPanoramaSageMakerRolePolicy

Deskripsi: Memungkinkan Amazon SageMaker mengelola objek dalam bucket yang dibuat untuk digunakan dengan AWS Panorama.

`AWSPanoramaSageMakerRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPanoramaSageMakerRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Desember 2020, 13:13 UTC
- Waktu teredit: 01 Desember 2020, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucket*"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPanoramaServiceLinkedRolePolicy

Deskripsi: Memungkinkan AWS Panorama untuk mengelola sumber daya di AWS IoT, Manajer AWS Rahasia dan AWS Panorama.

`AWSPanoramaServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 20 Oktober 2021, 12:12 UTC
- Waktu teredit: 20 Oktober 2021, 12:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing",
        "iot:DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot:DeleteCertificate",
        "iot:AttachPrincipalPolicy",
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*",
        "arn:aws:iot:*:*:cert/*"
```

```
      ]
    },
    {
      "Sid" : "PanoramaIoTCreateCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreatePolicyAndVersionAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreatePolicy",
        "iot:CreatePolicyVersion",
        "iot:AttachPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeJobExecution",
        "iot:CreateJob",
        "iot:DeleteJob"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:job/panorama*",
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "PanoramaReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "panorama:Describe*",
        "panorama:List*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:panorama*",
        "arn:aws:secretsmanager:*:*:secret:Panorama*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPanoramaServiceRolePolicy

Deskripsi: Men AWS gizinkan Panorama mengelola sumber daya di Amazon S3, AWS AWS IoT GreenGrass, IoT, AWS Lambda SageMaker, Amazon, dan Amazon CloudWatch Logs, dan meneruskan peran layanan ke AWS IoT, AWS IoT GreenGrass, dan Amazon SageMaker.

`AWSPanoramaServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPanoramaServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Desember 2020, 13:14 UTC
- Waktu teredit: 01 Desember 2020, 13:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing",
        "iot:DeleteThingShadow",
        "iot:DescribeThing",
```

```
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot:DeleteCertificate",
        "iot:AttachPrincipalPolicy",
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreateCertificateAndPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreatePolicyVersionAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreatePolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/panorama*"
      ]
```

```
    },
    {
      "Sid" : "PanoramaIoTJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeJobExecution",
        "iot:CreateJob",
        "iot:DeleteJob"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:job/panorama*",
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaAccess",
      "Effect" : "Allow",
      "Action" : [
        "panorama:Describe*",
        "panorama:List*",
        "panorama:Get*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:DeleteBucket",
```

```
        "s3:ListBucket",
        "s3:GetBucket*",
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIAMPassSageMakerRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaSageMakerRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaSageMakerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PanoramaIAMPassGreengrassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaGreengrassGroupRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaGreengrassGroupRole",
        "arn:aws:iam::*:role/AWSPanoramaGreengrassRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaGreengrassRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "greengrass.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "PanoramaIAMPassIoTRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaApplianceRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaApplianceRole"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "iot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PanoramaGreenGrassAccess",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:AssociateRoleToGroup",
        "greengrass:AssociateServiceRoleToAccount",
        "greengrass:CreateResourceDefinition",
        "greengrass:CreateResourceDefinitionVersion",
        "greengrass:CreateCoreDefinition",
        "greengrass:CreateCoreDefinitionVersion",
        "greengrass:CreateDeployment",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:CreateGroup",
        "greengrass:CreateGroupCertificateAuthority",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateLoggerDefinition",
        "greengrass:CreateLoggerDefinitionVersion",
        "greengrass:CreateSubscriptionDefinition",
        "greengrass:CreateSubscriptionDefinitionVersion",
        "greengrass:DeleteCoreDefinition",
        "greengrass:DeleteFunctionDefinition",
        "greengrass:DeleteResourceDefinition",
        "greengrass:DeleteGroup",
        "greengrass:DeleteLoggerDefinition",
        "greengrass:DeleteSubscriptionDefinition",
```

```
        "greengrass:DisassociateRoleFromGroup",
        "greengrass:DisassociateServiceRoleFromAccount",
        "greengrass:GetAssociatedRole",
        "greengrass:GetConnectivityInfo",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetDeviceDefinition",
        "greengrass:GetDeviceDefinitionVersion",
        "greengrass:GetFunctionDefinition",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupCertificateAuthority",
        "greengrass:GetGroupCertificateConfiguration",
        "greengrass:GetGroupVersion",
        "greengrass:GetLoggerDefinition",
        "greengrass:GetLoggerDefinitionVersion",
        "greengrass:GetResourceDefinition",
        "greengrass:GetServiceRoleForAccount",
        "greengrass:GetSubscriptionDefinition",
        "greengrass:GetSubscriptionDefinitionVersion",
        "greengrass:ListCoreDefinitionVersions",
        "greengrass:ListCoreDefinitions",
        "greengrass:ListDeployments",
        "greengrass:ListDeviceDefinitionVersions",
        "greengrass:ListDeviceDefinitions",
        "greengrass:ListFunctionDefinitionVersions",
        "greengrass:ListFunctionDefinitions",
        "greengrass:ListGroupCertificateAuthorities",
        "greengrass:ListGroupVersions",
        "greengrass:ListGroups",
        "greengrass:ListLoggerDefinitionVersions",
        "greengrass:ListLoggerDefinitions",
        "greengrass:ListSubscriptionDefinitionVersions",
        "greengrass:ListSubscriptionDefinitions",
        "greengrass:ResetDeployments",
        "greengrass:UpdateConnectivityInfo",
        "greengrass:UpdateCoreDefinition",
        "greengrass:UpdateDeviceDefinition",
        "greengrass:UpdateFunctionDefinition",
        "greengrass:UpdateGroup",
        "greengrass:UpdateGroupCertificateConfiguration",
        "greengrass:UpdateLoggerDefinition",
        "greengrass:UpdateSubscriptionDefinition",
```

```
        "greengrass:UpdateResourceDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaLambdaUsersFunctionAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*"
      ]
    },
    {
      "Sid" : "PanoramaSageMakerWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:CreateCompilationJob",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:StopCompilationJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/panorama*",
        "arn:aws:sagemaker:*:*:compilation-job/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaSageMakerListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListCompilationJobs"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "PanoramaSageMakerReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
      ]
    },
    {
      "Sid" : "PanoramaCWLogsAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachPolicy",
        "iot:CreateRoleAlias"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/panorama*",
        "arn:aws:iot:*:*:rolealias/panorama*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPartnerCentralChannelHandshakeApprovalManagement

Deskripsi: Menyediakan akses yang diperlukan untuk kegiatan manajemen persetujuan jabat tangan saluran.

`AWSPartnerCentralChannelHandshakeApprovalManagement`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPartnerCentralChannelHandshakeApprovalManagement` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 November 2025, 16:34 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralChannelHandshakeApprovalManagement`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ChannelHandshakeManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListChannelHandshakes",
        "partnercentral:AcceptChannelHandshake",
        "partnercentral:RejectChannelHandshake"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
```

```
            "Sandbox"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPartnerCentralChannelManagement

Deskripsi: Menyediakan akses yang diperlukan untuk aktivitas manajemen saluran.

`AWSPartnerCentralChannelManagement`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPartnerCentralChannelManagement` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 November 2025, 16:34 UTC
- Waktu teredit: 14 Februari 2026, 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralChannelManagement`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ChannelManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateProgramManagementAccount",
        "partnercentral:UpdateProgramManagementAccount",
        "partnercentral:DeleteProgramManagementAccount",
        "partnercentral:ListProgramManagementAccounts",
        "partnercentral:GetProgramManagementAccount",
        "partnercentral:CreateRelationship",
        "partnercentral:UpdateRelationship",
        "partnercentral:DeleteRelationship",
        "partnercentral:GetRelationship",
        "partnercentral:ListRelationships",
        "partnercentral:CreateChannelHandshake",
        "partnercentral:AcceptChannelHandshake",
        "partnercentral:RejectChannelHandshake",
        "partnercentral:CancelChannelHandshake",
        "partnercentral:ListChannelHandshakes"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "ChannelBillingTransferRoleAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferManagement",
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferReadOnly"
      ]
    },
    {
      "Sid" : "TaggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:TagResource",
        "partnercentral:UntagResource",
        "partnercentral:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/program-management-account/*",
        "arn:aws:partnercentral:*:*:catalog/*/channel-handshake/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" : "ChannelUser"
        }
      }
    },
    {
      "Sid" : "PartnerDashboardAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "partnercentral:GetPartnerDashboard"
      ],
      "Resource" : [
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/Resell_V1/Dashboard/*"
      ]
    },
    {
      "Sid" : "PartnerResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners",
        "partnercentral:GetPartner"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPartnerCentralFullAccess

Deskripsi: Menyediakan akses penuh ke Pusat AWS Mitra dan terkait Layanan AWS.

`AWSPartnerCentralFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPartnerCentralFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 November 2024, 23:33 UTC
- Waktu teredit: 12 Maret 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralFullAccess`

Versi kebijakan

Versi kebijakan: v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PassAWSPartnerCentralRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/PartnerCentralRoleFor*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "partnercentral-account-management.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PartnerUserRoleAssociation",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "Partnercentral-account-management:AssociatePartnerUser",
        "Partnercentral-account-management:DisassociatePartnerUser"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "VerificationAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:StartVerification",
        "partnercentral:GetVerification"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassAWSPartnerCentralSnapshotJobRole",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "resource-snapshot-job.partnercentral-
selling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerCentralMarketingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessMarketingCentral"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ChannelBillingTransferRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferManagement",
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferReadOnly"
      ]
    },
    {
      "Sid" : "PartnerCentralEphemeralWriteS3Access",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-
files/${aws:PrincipalAccount}/*"
    },
    {
      "Sid" : "SupportAccess",
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase",
        "support:DescribeCases",
        "support:AddCommunicationToCase",
        "support:ResolveCase",
        "support:AddAttachmentsToSet",
        "support:DescribeCommunications"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListEntitiesAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeEntityAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Solution/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/OfferSet/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Offer/*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceAgreementsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
```

```
        "aws-marketplace:DescribeAgreement"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerCentralAgentsSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:UseSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        },
        "Bool" : {
          "aws:IsMcpServiceAction" : "true"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPartnerCentralMarketingManagement

Deskripsi: Menyediakan akses yang diperlukan untuk kegiatan pemasaran.

`AWSPartnerCentralMarketingManagement`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPartnerCentralMarketingManagement` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2025, 00:34 UTC
- Waktu teredit: 14 Februari 2026, 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralMarketingManagement`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PartnerCentralMarketingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessMarketingCentral"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" :
 "MarketingStaff"
        }
      }
    },
    {
      "Sid" : "PartnerDiscoveryAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:SearchPartnerProfiles",
        "partnercentral:GetPartnerProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerProfileAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:StartProfileUpdateTask",
        "partnercentral:GetProfileUpdateTask",
        "partnercentral:CancelProfileUpdateTask",
```

```
        "partnercentral:PutProfileVisibility",
        "partnercentral:GetProfileVisibility"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/partner/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners",
        "partnercentral:GetPartner"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerCentralEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-
files/${aws:PrincipalAccount}/*"
    },
    {
      "Sid" : "PartnerDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetPartnerDashboard"
```

```
      ],
      "Resource" : [
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/MarketingCampaign_V1/
Dashboard/*"
      ]
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPartnerCentralOpportunityManagement

Deskripsi: Menyediakan akses yang diperlukan untuk kegiatan manajemen peluang.

`AWSPartnerCentralOpportunityManagement`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPartnerCentralOpportunityManagement` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 November 2024, 19:09 UTC
- Waktu teredit: 16 Juni 2026, 13:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralOpportunityManagement`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OpportunityManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:AcceptEngagementInvitation",
        "partnercentral:AssignOpportunity",
        "partnercentral:AssociateOpportunity",
        "partnercentral:CreateEngagement",
        "partnercentral:CreateEngagementContext",
        "partnercentral:CreateEngagementInvitation",
        "partnercentral:CreateOpportunity",
        "partnercentral:CreateResourceSnapshot",
        "partnercentral:CreateResourceSnapshotJob",
        "partnercentral:DeleteResourceSnapshotJob",
        "partnercentral:DisassociateOpportunity",
        "partnercentral:GetAwsOpportunitySummary",
        "partnercentral:GetEngagement",
        "partnercentral:GetEngagementInvitation",
        "partnercentral:GetOpportunity",
        "partnercentral:GetProspectingFromEngagementTask",
```

```
        "partnercentral:GetResourceSnapshot",
        "partnercentral:GetResourceSnapshotJob",
        "partnercentral:ListEngagementByAcceptingInvitationTasks",
        "partnercentral:ListEngagementFromOpportunityTasks",
        "partnercentral:ListEngagementInvitations",
        "partnercentral:ListEngagementMembers",
        "partnercentral:ListEngagementResourceAssociations",
        "partnercentral:ListEngagements",
        "partnercentral:ListOpportunities",
        "partnercentral:ListOpportunityFromEngagementTasks",
        "partnercentral:ListProspectingFromEngagementTasks",
        "partnercentral:ListResourceSnapshotJobs",
        "partnercentral:ListResourceSnapshots",
        "partnercentral:ListSolutions",
        "partnercentral:RejectEngagementInvitation",
        "partnercentral:StartEngagementByAcceptingInvitationTask",
        "partnercentral:StartEngagementFromOpportunityTask",
        "partnercentral:StartOpportunityFromEngagementTask",
        "partnercentral:StartProspectingFromEngagementTask",
        "partnercentral:StartResourceSnapshotJob",
        "partnercentral:StopResourceSnapshotJob",
        "partnercentral:SubmitOpportunity",
        "partnercentral:UpdateEngagementContext",
        "partnercentral:UpdateOpportunity"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "ListingAWSMarketplaceEntities",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AWSMarketplaceEntityAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Solution/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/OfferSet/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Offer/*"
      ]
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" : "AceManager"
        }
      }
    },
    {
      "Sid" : "PartnerDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetPartnerDashboard"
      ],
      "Resource" : [
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/Opportunity_V1/Dashboard/
*",
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/Engagement_V1/Dashboard/*"
      ]
    },
    {
      "Sid" : "CollaborationChannelAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateCollaborationChannelRequest",
        "partnercentral:ListCollaborationChannels",
        "partnercentral:GetCollaborationChannel",
        "partnercentral:CreateCollaborationChannelMembers"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners",
        "partnercentral:GetPartner"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "TaggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:TagResource",
        "partnercentral:UntagResource",
        "partnercentral:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/opportunity/*",
        "arn:aws:partnercentral:*:*:catalog/*/resource-snapshot-job/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerCentralAgentsSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:UseSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        },
        "Bool" : {
          "aws:IsMcpServiceAction" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPartnerCentralRevenueAttributionManagement

Deskripsi: Menyediakan akses yang diperlukan untuk kegiatan manajemen atribusi pendapatan.

`AWSPartnerCentralRevenueAttributionManagement`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPartnerCentralRevenueAttributionManagement` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Juni 2026, 19:12 UTC
- Waktu teredit: 30 Juni 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralRevenueAttributionManagement`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RevenueMeasurementCreation",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateRevenueAttribution",
        "partnercentral:CreateMarketplaceRevenueShare",
        "partnercentral:CreateMarketplaceRevenueShareAllocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
```

```
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "RevenueMeasurementListing",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListRevenueAttributions",
        "partnercentral:ListRevenueAttributionAllocations",
        "partnercentral:ListMarketplaceRevenueShares",
        "partnercentral:ListMarketplaceRevenueShareAllocations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "RevenueAttributionManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetRevenueAttribution",
        "partnercentral:UpdateRevenueAttribution",
        "partnercentral:GetRevenueAttributionAllocation",
        "partnercentral:StartRevenueAttributionAllocationsTask",
        "partnercentral:GetRevenueAttributionAllocationsTask"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/revenue-attribution/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "MarketplaceRevenueShareManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetMarketplaceRevenueShare",
        "partnercentral:GetMarketplaceRevenueShareAllocation",
        "partnercentral:UpdateMarketplaceRevenueShareAllocation"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/marketplace-revenue-share/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "TaggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:TagResource",
        "partnercentral:UntagResource",
        "partnercentral:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/revenue-attribution/*",
        "arn:aws:partnercentral:*:*:catalog/*/marketplace-revenue-share/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "OpportunityListing",
      "Effect" : "Allow",
      "Action" : [
```

```
        "partnercentral:ListOpportunities"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "OpportunityAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetOpportunity"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/opportunity/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerListing",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "PartnerResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetPartner"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/partner/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "ListingAWSMarketplaceEntities",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceEntityAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Offer/*"
      ]
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPartnerCentralSandboxFullAccess

Deskripsi: Menyediakan akses yang diperlukan untuk pengujian pengembang di katalog Sandbox.

`AWSPartnerCentralSandboxFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPartnerCentralSandboxFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 November 2024, 19:10 UTC
- Waktu teredit: 12 Maret 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralSandboxFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSPartnerCentralSandboxAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : "Sandbox"
        }
      }
    },
    {
      "Sid" : "PartnerCentralAgentsSandboxSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:UseSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : "Sandbox"
        },
        "Bool" : {
          "aws:IsMcpServiceAction" : "true"
        }
      }
    },
    {
      "Sid" : "PassAWSPartnerCentralSnapshotJobRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "resource-snapshot-job.partnercentral-
selling.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy

Deskripsi: Menyediakan akses ResourceSnapshotJob ke untuk membaca sumber daya dan memotretnya dalam keterlibatan target.

`AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 Desember 2024, 18:21 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateResourceSnapshot"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*::catalog/AWS/engagement/*",
        "arn:aws:partnercentral:*::catalog/Sandbox/engagement/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetOpportunity"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/AWS/opportunity/*",
        "arn:aws:partnercentral:*:*:catalog/Sandbox/opportunity/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPartnerLedSupportReadOnlyAccess

Deskripsi: Kebijakan ini dapat digunakan untuk memberikan akses baca-saja ke API yang dapat membaca metadata layanan untuk layanan di Anda. Akun AWS Anda dapat menggunakan kebijakan ini untuk memberi mitra Anda di Program Partner-Led Dukungan akses ke layanan yang ditentukan di bagian detail izin di bawah ini.

`AWSPartnerLedSupportReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPartnerLedSupportReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 November 2024, 20:06 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerLedSupportReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
```

```
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/domainnames/*/apimappings/*",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models/*/default_template",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration/responses/
*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/responses/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*/sdks/*",
```

```
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:describeCertificateAuthority",
        "acm-pca:describeCertificateAuthorityAuditReport",
        "acm-pca:getCertificate",
        "acm-pca:getCertificateAuthorityCertificate",
        "acm-pca:getCertificateAuthorityCsr",
        "acm-pca:listCertificateAuthorities",
        "acm-pca:listTags",
        "acm:describeCertificate",
        "acm:getAccountConfiguration",
        "acm:getCertificate",
        "acm:listCertificates",
        "acm:listTagsForCertificate",
        "athena:batchGetNamedQuery",
        "athena:batchGetQueryExecution",
        "athena:getCalculationExecution",
        "athena:getCalculationExecutionStatus",
        "athena:getDataCatalog",
        "athena:getNamedQuery",
        "athena:getNotebookMetadata",
        "athena:getQueryExecution",
        "athena:getQueryRuntimeStatistics",
        "athena:getSession",
        "athena:getSessionStatus",
        "athena:getWorkGroup",
        "athena:listApplicationDPUSizes",
        "athena:listCalculationExecutions",
        "athena:listDataCatalogs",
        "athena:listEngineVersions",
        "athena:listExecutors",
        "athena:listNamedQueries",
        "athena:listNotebookMetadata",
```

```
        "athena:listNotebookSessions",
        "athena:listQueryExecutions",
        "athena:listSessions",
        "athena:listTagsForResource",
        "athena:listWorkGroups",
        "backup-gateway:getGateway",
        "backup-gateway:getHypervisor",
        "backup-gateway:getHypervisorPropertyMappings",
        "backup-gateway:getVirtualMachine",
        "backup-gateway:listGateways",
        "backup-gateway:listHypervisors",
        "backup-gateway:listVirtualMachines",
        "backup:describeBackupJob",
        "backup:describeBackupVault",
        "backup:describeCopyJob",
        "backup:describeFramework",
        "backup:describeGlobalSettings",
        "backup:describeProtectedResource",
        "backup:describeRecoveryPoint",
        "backup:describeRegionSettings",
        "backup:describeReportJob",
        "backup:describeReportPlan",
        "backup:describeRestoreJob",
        "backup:getBackupPlan",
        "backup:getBackupPlanFromJSON",
        "backup:getBackupPlanFromTemplate",
        "backup:getBackupSelection",
        "backup:getBackupVaultAccessPolicy",
        "backup:getBackupVaultNotifications",
        "backup:getLegalHold",
        "backup:getRecoveryPointRestoreMetadata",
        "backup:getRestoreJobMetadata",
        "backup:getRestoreTestingInferredMetadata",
        "backup:getRestoreTestingPlan",
        "backup:getRestoreTestingSelection",
        "backup:getSupportedResourceTypes",
        "backup:listBackupJobs",
        "backup:listBackupPlanTemplates",
        "backup:listBackupPlanVersions",
        "backup:listBackupPlans",
        "backup:listBackupSelections",
        "backup:listBackupVaults",
        "backup:listCopyJobs",
        "backup:listFrameworks",
```

```
        "backup:listLegalHolds",
        "backup:listProtectedResources",
        "backup:listRecoveryPointsByBackupVault",
        "backup:listRecoveryPointsByLegalHold",
        "backup:listRecoveryPointsByResource",
        "backup:listReportJobs",
        "backup:listReportPlans",
        "backup:listRestoreJobs",
        "backup:listRestoreJobsByProtectedResource",
        "backup:listRestoreTestingPlans",
        "backup:listRestoreTestingSelections",
        "backup:listTags",
        "cloudformation:batchDescribeTypeConfigurations",
        "cloudformation:describeAccountLimits",
        "cloudformation:describeChangeSet",
        "cloudformation:describeChangeSetHooks",
        "cloudformation:describePublisher",
        "cloudformation:describeStackEvents",
        "cloudformation:describeStackInstance",
        "cloudformation:describeStackResource",
        "cloudformation:describeStackResources",
        "cloudformation:describeStackSet",
        "cloudformation:describeStackSetOperation",
        "cloudformation:describeStacks",
        "cloudformation:describeType",
        "cloudformation:describeTypeRegistration",
        "cloudformation:estimateTemplateCost",
        "cloudformation:getStackPolicy",
        "cloudformation:getTemplate",
        "cloudformation:getTemplateSummary",
        "cloudformation:listChangeSets",
        "cloudformation:listExports",
        "cloudformation:listImports",
        "cloudformation:listStackInstances",
        "cloudformation:listStackResources",
        "cloudformation:listStackSetOperationResults",
        "cloudformation:listStackSetOperations",
        "cloudformation:listStackSets",
        "cloudformation:listStacks",
        "cloudformation:listTypeRegistrations",
        "cloudformation:listTypeVersions",
        "cloudformation:listTypes",
        "cloudfront:describeFunction",
        "cloudfront:getCachePolicy",
```

```
        "cloudfront:getCachePolicyConfig",
        "cloudfront:getCloudFrontOriginAccessIdentity",
        "cloudfront:getCloudFrontOriginAccessIdentityConfig",
        "cloudfront:getContinuousDeploymentPolicy",
        "cloudfront:getContinuousDeploymentPolicyConfig",
        "cloudfront:getDistribution",
        "cloudfront:getDistributionConfig",
        "cloudfront:getInvalidation",
        "cloudfront:getKeyGroup",
        "cloudfront:getKeyGroupConfig",
        "cloudfront:getMonitoringSubscription",
        "cloudfront:getOriginAccessControl",
        "cloudfront:getOriginAccessControlConfig",
        "cloudfront:getOriginRequestPolicy",
        "cloudfront:getOriginRequestPolicyConfig",
        "cloudfront:getPublicKey",
        "cloudfront:getPublicKeyConfig",
        "cloudfront:getRealtimeLogConfig",
        "cloudfront:getResponseHeadersPolicy",
        "cloudfront:getResponseHeadersPolicyConfig",
        "cloudfront:getStreamingDistribution",
        "cloudfront:getStreamingDistributionConfig",
        "cloudfront:listCachePolicies",
        "cloudfront:listCloudFrontOriginAccessIdentities",
        "cloudfront:listContinuousDeploymentPolicies",
        "cloudfront:listDistributions",
        "cloudfront:listDistributionsByCachePolicyId",
        "cloudfront:listDistributionsByKeyGroup",
        "cloudfront:listDistributionsByOriginRequestPolicyId",
        "cloudfront:listDistributionsByRealtimeLogConfig",
        "cloudfront:listDistributionsByResponseHeadersPolicyId",
        "cloudfront:listDistributionsByWebACLId",
        "cloudfront:listFunctions",
        "cloudfront:listInvalidations",
        "cloudfront:listKeyGroups",
        "cloudfront:listOriginAccessControls",
        "cloudfront:listOriginRequestPolicies",
        "cloudfront:listPublicKeys",
        "cloudfront:listRealtimeLogConfigs",
        "cloudfront:listResponseHeadersPolicies",
        "cloudfront:listStreamingDistributions",
        "cloudtrail:describeTrails",
        "cloudtrail:getEventSelectors",
        "cloudtrail:lookupEvents",
```

```
        "cloudwatch:describeAlarmHistory",
        "cloudwatch:describeAlarms",
        "cloudwatch:describeAlarmsForMetric",
        "cloudwatch:describeAnomalyDetectors",
        "cloudwatch:describeInsightRules",
        "cloudwatch:getDashboard",
        "cloudwatch:getInsightRuleReport",
        "cloudwatch:getMetricData",
        "cloudwatch:getMetricStatistics",
        "cloudwatch:getMetricStream",
        "cloudwatch:listDashboards",
        "cloudwatch:listManagedInsightRules",
        "cloudwatch:listMetricStreams",
        "cloudwatch:listMetrics",
        "codepipeline:getPipeline",
        "codepipeline:getPipelineState",
        "codepipeline:listActionTypes",
        "codepipeline:listPipelineExecutions",
        "codepipeline:listPipelines",
        "cognito-identity:describeIdentityPool",
        "cognito-identity:getIdentityPoolRoles",
        "cognito-identity:listIdentities",
        "cognito-identity:listIdentityPools",
        "cognito-idp:describeIdentityProvider",
        "cognito-idp:describeResourceServer",
        "cognito-idp:describeRiskConfiguration",
        "cognito-idp:describeUserImportJob",
        "cognito-idp:describeUserPool",
        "cognito-idp:describeUserPoolClient",
        "cognito-idp:describeUserPoolDomain",
        "cognito-idp:getGroup",
        "cognito-idp:getUICustomization",
        "cognito-idp:getUserPoolMfaConfig",
        "cognito-idp:listGroups",
        "cognito-idp:listIdentityProviders",
        "cognito-idp:listResourceServers",
        "cognito-idp:listUserImportJobs",
        "cognito-idp:listUserPoolClients",
        "cognito-idp:listUserPools",
        "cognito-sync:describeDataset",
        "cognito-sync:describeIdentityPoolUsage",
        "cognito-sync:describeIdentityUsage",
        "cognito-sync:getCognitoEvents",
        "cognito-sync:getIdentityPoolConfiguration",
```

```
        "cognito-sync:listDatasets",
        "cognito-sync:listIdentityPoolUsage",
        "connect:describeContact",
        "connect:describePhoneNumber",
        "connect:describeQuickConnect",
        "connect:describeUser",
        "connect:getCurrentMetricData",
        "connect:getMetricData",
        "connect:listContactEvaluations",
        "connect:listEvaluationFormVersions",
        "connect:listEvaluationForms",
        "connect:listPhoneNumbersV2",
        "connect:listQuickConnects",
        "connect:listRoutingProfiles",
        "connect:listSecurityProfiles",
        "connect:listUsers",
        "connect:listViewVersions",
        "connect:listViews",
        "directconnect:describeConnectionLoa",
        "directconnect:describeConnections",
        "directconnect:describeConnectionsOnInterconnect",
        "directconnect:describeCustomerMetadata",
        "directconnect:describeDirectConnectGatewayAssociationProposals",
        "directconnect:describeDirectConnectGatewayAssociations",
        "directconnect:describeDirectConnectGatewayAttachments",
        "directconnect:describeDirectConnectGateways",
        "directconnect:describeHostedConnections",
        "directconnect:describeInterconnectLoa",
        "directconnect:describeInterconnects",
        "directconnect:describeLags",
        "directconnect:describeLoa",
        "directconnect:describeLocations",
        "directconnect:describeRouterConfiguration",
        "directconnect:describeVirtualGateways",
        "directconnect:describeVirtualInterfaces",
        "dms:describeAccountAttributes",
        "dms:describeApplicableIndividualAssessments",
        "dms:describeConnections",
        "dms:describeEndpointSettings",
        "dms:describeEndpointTypes",
        "dms:describeEndpoints",
        "dms:describeEventCategories",
        "dms:describeEventSubscriptions",
        "dms:describeEvents",
```

```
        "dms:describeFleetAdvisorCollectors",
        "dms:describeFleetAdvisorDatabases",
        "dms:describeFleetAdvisorLsaAnalysis",
        "dms:describeFleetAdvisorSchemaObjectSummary",
        "dms:describeFleetAdvisorSchemas",
        "dms:describeOrderableReplicationInstances",
        "dms:describePendingMaintenanceActions",
        "dms:describeRefreshSchemasStatus",
        "dms:describeReplicationInstanceTaskLogs",
        "dms:describeReplicationInstances",
        "dms:describeReplicationSubnetGroups",
        "dms:describeReplicationTaskAssessmentResults",
        "dms:describeReplicationTaskAssessmentRuns",
        "dms:describeReplicationTaskIndividualAssessments",
        "dms:describeReplicationTasks",
        "dms:describeSchemas",
        "dms:describeTableStatistics",
        "ds:describeClientAuthenticationSettings",
        "ds:describeConditionalForwarders",
        "ds:describeDirectories",
        "ds:describeDomainControllers",
        "ds:describeEventTopics",
        "ds:describeLDAPSSettings",
        "ds:describeSharedDirectories",
        "ds:describeSnapshots",
        "ds:describeTrusts",
        "ds:getDirectoryLimits",
        "ds:getSnapshotLimits",
        "ds:listIpRoutes",
        "ds:listSchemaExtensions",
        "ds:listTagsForResource",
        "ec2:describeAccountAttributes",
        "ec2:describeAddressTransfers",
        "ec2:describeAddresses",
        "ec2:describeAddressesAttribute",
        "ec2:describeAggregateIdFormat",
        "ec2:describeAvailabilityZones",
        "ec2:describeBundleTasks",
        "ec2:describeByoipCidrs",
        "ec2:describeCapacityReservationFleets",
        "ec2:describeCapacityReservations",
        "ec2:describeCarrierGateways",
        "ec2:describeClassicLinkInstances",
        "ec2:describeClientVpnAuthorizationRules",
```

```
        "ec2:describeClientVpnConnections",
        "ec2:describeClientVpnEndpoints",
        "ec2:describeClientVpnRoutes",
        "ec2:describeClientVpnTargetNetworks",
        "ec2:describeCoipPools",
        "ec2:describeConversionTasks",
        "ec2:describeCustomerGateways",
        "ec2:describeDhcpOptions",
        "ec2:describeEgressOnlyInternetGateways",
        "ec2:describeExportImageTasks",
        "ec2:describeExportTasks",
        "ec2:describeFastLaunchImages",
        "ec2:describeFastSnapshotRestores",
        "ec2:describeFleetHistory",
        "ec2:describeFleetInstances",
        "ec2:describeFleets",
        "ec2:describeFlowLogs",
        "ec2:describeFpgaImageAttribute",
        "ec2:describeFpgaImages",
        "ec2:describeHostReservationOfferings",
        "ec2:describeHostReservations",
        "ec2:describeHosts",
        "ec2:describeIamInstanceProfileAssociations",
        "ec2:describeIdFormat",
        "ec2:describeIdentityIdFormat",
        "ec2:describeImageAttribute",
        "ec2:describeImages",
        "ec2:describeImportImageTasks",
        "ec2:describeImportSnapshotTasks",
        "ec2:describeInstanceAttribute",
        "ec2:describeInstanceCreditSpecifications",
        "ec2:describeInstanceEventNotificationAttributes",
        "ec2:describeInstanceEventWindows",
        "ec2:describeInstanceStatus",
        "ec2:describeInstanceTypeOfferings",
        "ec2:describeInstanceTypes",
        "ec2:describeInstances",
        "ec2:describeInternetGateways",
        "ec2:describeIpamPools",
        "ec2:describeIpamScopes",
        "ec2:describeIpams",
        "ec2:describeIpv6Pools",
        "ec2:describeKeyPairs",
        "ec2:describeLaunchTemplateVersions",
```

```
        "ec2:describeLaunchTemplates",
        "ec2:describeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:describeLocalGatewayRouteTableVpcAssociations",
        "ec2:describeLocalGatewayRouteTables",
        "ec2:describeLocalGatewayVirtualInterfaceGroups",
        "ec2:describeLocalGatewayVirtualInterfaces",
        "ec2:describeLocalGateways",
        "ec2:describeManagedPrefixLists",
        "ec2:describeMovingAddresses",
        "ec2:describeNatGateways",
        "ec2:describeNetworkAcls",
        "ec2:describeNetworkInterfaceAttribute",
        "ec2:describeNetworkInterfaces",
        "ec2:describePlacementGroups",
        "ec2:describePrefixLists",
        "ec2:describePrincipalIdFormat",
        "ec2:describePublicIpv4Pools",
        "ec2:describeRegions",
        "ec2:describeReservedInstances",
        "ec2:describeReservedInstancesListings",
        "ec2:describeReservedInstancesModifications",
        "ec2:describeReservedInstancesOfferings",
        "ec2:describeRouteTables",
        "ec2:describeScheduledInstanceAvailability",
        "ec2:describeScheduledInstances",
        "ec2:describeSecurityGroupReferences",
        "ec2:describeSecurityGroupRules",
        "ec2:describeSecurityGroups",
        "ec2:describeSnapshotAttribute",
        "ec2:describeSnapshotTierStatus",
        "ec2:describeSnapshots",
        "ec2:describeSpotDatafeedSubscription",
        "ec2:describeSpotFleetInstances",
        "ec2:describeSpotFleetRequestHistory",
        "ec2:describeSpotFleetRequests",
        "ec2:describeSpotInstanceRequests",
        "ec2:describeSpotPriceHistory",
        "ec2:describeStaleSecurityGroups",
        "ec2:describeStoreImageTasks",
        "ec2:describeSubnets",
        "ec2:describeTags",
        "ec2:describeTrafficMirrorFilters",
        "ec2:describeTrafficMirrorSessions",
        "ec2:describeTrafficMirrorTargets",
```

```
        "ec2:describeTransitGatewayAttachments",
        "ec2:describeTransitGatewayConnectPeers",
        "ec2:describeTransitGatewayMulticastDomains",
        "ec2:describeTransitGatewayPeeringAttachments",
        "ec2:describeTransitGatewayPolicyTables",
        "ec2:describeTransitGatewayRouteTableAnnouncements",
        "ec2:describeTransitGatewayRouteTables",
        "ec2:describeTransitGatewayVpcAttachments",
        "ec2:describeTransitGateways",
        "ec2:describeVerifiedAccessEndpoints",
        "ec2:describeVerifiedAccessGroups",
        "ec2:describeVerifiedAccessInstances",
        "ec2:describeVerifiedAccessTrustProviders",
        "ec2:describeVolumeAttribute",
        "ec2:describeVolumeStatus",
        "ec2:describeVolumes",
        "ec2:describeVolumesModifications",
        "ec2:describeVpcAttribute",
        "ec2:describeVpcClassicLink",
        "ec2:describeVpcClassicLinkDnsSupport",
        "ec2:describeVpcEndpointConnectionNotifications",
        "ec2:describeVpcEndpointConnections",
        "ec2:describeVpcEndpointServiceConfigurations",
        "ec2:describeVpcEndpointServicePermissions",
        "ec2:describeVpcEndpointServices",
        "ec2:describeVpcEndpoints",
        "ec2:describeVpcPeeringConnections",
        "ec2:describeVpcs",
        "ec2:describeVpnConnections",
        "ec2:describeVpnGateways",
        "ec2:getAssociatedIpv6PoolCidrs",
        "ec2:getCapacityReservationUsage",
        "ec2:getCoipPoolUsage",
        "ec2:getConsoleOutput",
        "ec2:getConsoleScreenshot",
        "ec2:getDefaultCreditSpecification",
        "ec2:getEbsDefaultKmsKeyId",
        "ec2:getEbsEncryptionByDefault",
        "ec2:getGroupsForCapacityReservation",
        "ec2:getHostReservationPurchasePreview",
        "ec2:getInstanceTypesFromInstanceRequirements",
        "ec2:getIpamAddressHistory",
        "ec2:getIpamPoolAllocations",
        "ec2:getIpamPoolCidrs",
```

```
        "ec2:getIpamResourceCidrs",
        "ec2:getLaunchTemplateData",
        "ec2:getManagedPrefixListAssociations",
        "ec2:getManagedPrefixListEntries",
        "ec2:getReservedInstancesExchangeQuote",
        "ec2:getSerialConsoleAccessStatus",
        "ec2:getSpotPlacementScores",
        "ec2:getSubnetCidrReservations",
        "ec2:getTransitGatewayMulticastDomainAssociations",
        "ec2:getTransitGatewayPrefixListReferences",
        "ec2:getVerifiedAccessEndpointPolicy",
        "ec2:getVerifiedAccessGroupPolicy",
        "ec2:listImagesInRecycleBin",
        "ec2:listSnapshotsInRecycleBin",
        "ec2:searchLocalGatewayRoutes",
        "ec2:searchTransitGatewayMulticastGroups",
        "ec2:searchTransitGatewayRoutes",
        "ecs:describeCapacityProviders",
        "ecs:describeClusters",
        "ecs:describeContainerInstances",
        "ecs:describeServices",
        "ecs:describeTaskDefinition",
        "ecs:describeTaskSets",
        "ecs:describeTasks",
        "ecs:getTaskProtection",
        "ecs:listAccountSettings",
        "ecs:listAttributes",
        "ecs:listClusters",
        "ecs:listContainerInstances",
        "ecs:listServices",
        "ecs:listServicesByNamespace",
        "ecs:listTagsForResource",
        "ecs:listTaskDefinitionFamilies",
        "ecs:listTaskDefinitions",
        "ecs:listTasks",
        "eks:describeAccessEntry",
        "eks:describeAddon",
        "eks:describeAddonConfiguration",
        "eks:describeAddonVersions",
        "eks:describeCluster",
        "eks:describeEksAnywhereSubscription",
        "eks:describeFargateProfile",
        "eks:describeIdentityProviderConfig",
        "eks:describeNodegroup",
```

```
        "eks:describePodIdentityAssociation",
        "eks:describeUpdate",
        "eks:listAccessEntries",
        "eks:listAccessPolicies",
        "eks:listAddons",
        "eks:listAssociatedAccessPolicies",
        "eks:listClusters",
        "eks:listEksAnywhereSubscriptions",
        "eks:listFargateProfiles",
        "eks:listIdentityProviderConfigs",
        "eks:listNodegroups",
        "eks:listPodIdentityAssociations",
        "eks:listUpdates",
        "elasticache:describeCacheClusters",
        "elasticache:describeCacheEngineVersions",
        "elasticache:describeCacheParameterGroups",
        "elasticache:describeCacheParameters",
        "elasticache:describeCacheSecurityGroups",
        "elasticache:describeCacheSubnetGroups",
        "elasticache:describeEngineDefaultParameters",
        "elasticache:describeEvents",
        "elasticache:describeGlobalReplicationGroups",
        "elasticache:describeReplicationGroups",
        "elasticache:describeReservedCacheNodes",
        "elasticache:describeReservedCacheNodesOfferings",
        "elasticache:describeServerlessCacheSnapshots",
        "elasticache:describeServerlessCaches",
        "elasticache:describeServiceUpdates",
        "elasticache:describeSnapshots",
        "elasticache:describeUpdateActions",
        "elasticache:describeUserGroups",
        "elasticache:describeUsers",
        "elasticache:listAllowedNodeTypeModifications",
        "elasticache:listTagsForResource",
        "elasticbeanstalk:checkDNSAvailability",
        "elasticbeanstalk:describeAccountAttributes",
        "elasticbeanstalk:describeApplicationVersions",
        "elasticbeanstalk:describeApplications",
        "elasticbeanstalk:describeConfigurationOptions",
        "elasticbeanstalk:describeEnvironmentHealth",
        "elasticbeanstalk:describeEnvironmentManagedActionHistory",
        "elasticbeanstalk:describeEnvironmentManagedActions",
        "elasticbeanstalk:describeEnvironmentResources",
        "elasticbeanstalk:describeEnvironments",
```

```
        "elasticbeanstalk:describeEvents",
        "elasticbeanstalk:describeInstancesHealth",
        "elasticbeanstalk:describePlatformVersion",
        "elasticbeanstalk:listAvailableSolutionStacks",
        "elasticbeanstalk:listPlatformBranches",
        "elasticbeanstalk:listPlatformVersions",
        "elasticbeanstalk:validateConfigurationSettings",
        "elasticfilesystem:describeAccessPoints",
        "elasticfilesystem:describeFileSystemPolicy",
        "elasticfilesystem:describeFileSystems",
        "elasticfilesystem:describeLifecycleConfiguration",
        "elasticfilesystem:describeMountTargetSecurityGroups",
        "elasticfilesystem:describeMountTargets",
        "elasticfilesystem:describeTags",
        "elasticfilesystem:listTagsForResource",
        "elasticloadbalancing:describeAccountLimits",
        "elasticloadbalancing:describeInstanceHealth",
        "elasticloadbalancing:describeListenerCertificates",
        "elasticloadbalancing:describeListeners",
        "elasticloadbalancing:describeLoadBalancerAttributes",
        "elasticloadbalancing:describeLoadBalancerPolicies",
        "elasticloadbalancing:describeLoadBalancerPolicyTypes",
        "elasticloadbalancing:describeLoadBalancers",
        "elasticloadbalancing:describeRules",
        "elasticloadbalancing:describeSSLPolicies",
        "elasticloadbalancing:describeTags",
        "elasticloadbalancing:describeTargetGroupAttributes",
        "elasticloadbalancing:describeTargetGroups",
        "elasticloadbalancing:describeTargetHealth",
        "elasticloadbalancing:describeTrustStoreAssociations",
        "elasticloadbalancing:describeTrustStoreRevocations",
        "elasticloadbalancing:describeTrustStores",
        "emr-containers:describeJobRun",
        "emr-containers:describeJobTemplate",
        "emr-containers:describeManagedEndpoint",
        "emr-containers:describeVirtualCluster",
        "emr-containers:listJobRuns",
        "emr-containers:listJobTemplates",
        "emr-containers:listManagedEndpoints",
        "emr-containers:listVirtualClusters",
        "emr-serverless:getApplication",
        "emr-serverless:getJobRun",
        "emr-serverless:listApplications",
        "es:describeDomain",
```

```
        "es:describeDomainAutoTunes",
        "es:describeDomainChangeProgress",
        "es:describeDomainConfig",
        "es:describeDomains",
        "es:describeDryRunProgress",
        "es:describeElasticsearchDomain",
        "es:describeElasticsearchDomainConfig",
        "es:describeElasticsearchDomains",
        "es:describeInboundConnections",
        "es:describeInstanceTypeLimits",
        "es:describeOutboundConnections",
        "es:describePackages",
        "es:describeReservedInstanceOfferings",
        "es:describeReservedInstances",
        "es:describeVpcEndpoints",
        "es:getCompatibleVersions",
        "es:getPackageVersionHistory",
        "es:getUpgradeHistory",
        "es:getUpgradeStatus",
        "es:listDomainNames",
        "es:listDomainsForPackage",
        "es:listInstanceTypeDetails",
        "es:listPackagesForDomain",
        "es:listScheduledActions",
        "es:listTags",
        "es:listVersions",
        "es:listVpcEndpointAccess",
        "es:listVpcEndpoints",
        "es:listVpcEndpointsForDomain",
        "events:describeApiDestination",
        "events:describeArchive",
        "events:describeConnection",
        "events:describeEndpoint",
        "events:describeEventBus",
        "events:describeEventSource",
        "events:describePartnerEventSource",
        "events:describeReplay",
        "events:describeRule",
        "events:listApiDestinations",
        "events:listArchives",
        "events:listConnections",
        "events:listEndpoints",
        "events:listEventBuses",
        "events:listEventSources",
```

```
        "events:listPartnerEventSourceAccounts",
        "events:listPartnerEventSources",
        "events:listReplays",
        "events:listRuleNamesByTarget",
        "events:listRules",
        "events:listTargetsByRule",
        "events:testEventPattern",
        "fsx:describeBackups",
        "fsx:describeDataRepositoryAssociations",
        "fsx:describeDataRepositoryTasks",
        "fsx:describeFileCaches",
        "fsx:describeFileSystems",
        "fsx:describeSnapshots",
        "fsx:describeStorageVirtualMachines",
        "fsx:describeVolumes",
        "fsx:listTagsForResource",
        "glue:batchGetBlueprints",
        "glue:batchGetCrawlers",
        "glue:batchGetDevEndpoints",
        "glue:batchGetJobs",
        "glue:batchGetPartition",
        "glue:batchGetTriggers",
        "glue:batchGetWorkflows",
        "glue:checkSchemaVersionValidity",
        "glue:getBlueprint",
        "glue:getBlueprintRun",
        "glue:getBlueprintRuns",
        "glue:getCatalogImportStatus",
        "glue:getClassifier",
        "glue:getClassifiers",
        "glue:getColumnStatisticsForPartition",
        "glue:getColumnStatisticsForTable",
        "glue:getCrawler",
        "glue:getCrawlerMetrics",
        "glue:getCrawlers",
        "glue:getCustomEntityType",
        "glue:getDataQualityResult",
        "glue:getDataQualityRuleRecommendationRun",
        "glue:getDataQualityRuleset",
        "glue:getDataQualityRulesetEvaluationRun",
        "glue:getDatabase",
        "glue:getDatabases",
        "glue:getDataflowGraph",
        "glue:getDevEndpoint",
```

```
        "glue:getDevEndpoints",
        "glue:getJob",
        "glue:getJobRun",
        "glue:getJobRuns",
        "glue:getJobs",
        "glue:getMLTaskRun",
        "glue:getMLTaskRuns",
        "glue:getMLTransform",
        "glue:getMLTransforms",
        "glue:getMapping",
        "glue:getPartition",
        "glue:getPartitionIndexes",
        "glue:getPartitions",
        "glue:getRegistry",
        "glue:getResourcePolicies",
        "glue:getResourcePolicy",
        "glue:getSchema",
        "glue:getSchemaByDefinition",
        "glue:getSchemaVersion",
        "glue:getSchemaVersionsDiff",
        "glue:getSession",
        "glue:getStatement",
        "glue:getTable",
        "glue:getTableVersions",
        "glue:getTables",
        "glue:getTrigger",
        "glue:getTriggers",
        "glue:getUserDefinedFunction",
        "glue:getUserDefinedFunctions",
        "glue:getWorkflow",
        "glue:getWorkflowRun",
        "glue:getWorkflowRuns",
        "glue:listCrawlers",
        "glue:listCrawls",
        "glue:listDataQualityResults",
        "glue:listDataQualityRuleRecommendationRuns",
        "glue:listDataQualityRulesetEvaluationRuns",
        "glue:listDataQualityRulesets",
        "glue:listDevEndpoints",
        "glue:listMLTransforms",
        "glue:listRegistries",
        "glue:listSchemaVersions",
        "glue:listSchemas",
        "glue:listSessions",
```

```
        "glue:listStatements",
        "glue:querySchemaVersionMetadata",
        "guardduty:getFindings",
        "guardduty:listDetectors",
        "guardduty:listFindings",
        "guardduty:listIPSets",
        "guardduty:listThreatIntelSets",
        "iam:getAccessKeyLastUsed",
        "iam:getAccountAuthorizationDetails",
        "iam:getAccountPasswordPolicy",
        "iam:getAccountSummary",
        "iam:getContextKeysForCustomPolicy",
        "iam:getContextKeysForPrincipalPolicy",
        "iam:getCredentialReport",
        "iam:getGroup",
        "iam:getGroupPolicy",
        "iam:getInstanceProfile",
        "iam:getLoginProfile",
        "iam:getOpenIDConnectProvider",
        "iam:getPolicy",
        "iam:getPolicyVersion",
        "iam:getRole",
        "iam:getRolePolicy",
        "iam:getSAMLProvider",
        "iam:getSSHPublicKey",
        "iam:getServerCertificate",
        "iam:getServiceLinkedRoleDeletionStatus",
        "iam:getUser",
        "iam:getUserPolicy",
        "iam:listAccessKeys",
        "iam:listAccountAliases",
        "iam:listAttachedGroupPolicies",
        "iam:listAttachedRolePolicies",
        "iam:listAttachedUserPolicies",
        "iam:listEntitiesForPolicy",
        "iam:listGroupPolicies",
        "iam:listGroups",
        "iam:listGroupsForUser",
        "iam:listInstanceProfiles",
        "iam:listInstanceProfilesForRole",
        "iam:listMFADevices",
        "iam:listOpenIDConnectProviders",
        "iam:listPolicies",
        "iam:listPolicyVersions",
```

```
        "iam:listRolePolicies",
        "iam:listRoles",
        "iam:listSAMLProviders",
        "iam:listSSHPublicKeys",
        "iam:listServerCertificates",
        "iam:listSigningCertificates",
        "iam:listUserPolicies",
        "iam:listUsers",
        "iam:listVirtualMFADevices",
        "kafka:describeCluster",
        "kafka:describeClusterOperation",
        "kafka:describeClusterOperationV2",
        "kafka:describeClusterV2",
        "kafka:describeConfiguration",
        "kafka:describeConfigurationRevision",
        "kafka:describeReplicator",
        "kafka:describeVpcConnection",
        "kafka:getBootstrapBrokers",
        "kafka:getClusterPolicy",
        "kafka:listClientVpcConnections",
        "kafka:listClusterOperations",
        "kafka:listClusterOperationsV2",
        "kafka:listClusters",
        "kafka:listClustersV2",
        "kafka:listConfigurationRevisions",
        "kafka:listConfigurations",
        "kafka:listNodes",
        "kafka:listReplicators",
        "kafka:listScramSecrets",
        "kafka:listVpcConnections",
        "kafkaconnect:describeConnector",
        "kafkaconnect:describeCustomPlugin",
        "kafkaconnect:describeWorkerConfiguration",
        "kafkaconnect:listConnectors",
        "kafkaconnect:listCustomPlugins",
        "kafkaconnect:listWorkerConfigurations",
        "lambda:getAccountSettings",
        "lambda:getAlias",
        "lambda:getCodeSigningConfig",
        "lambda:getEventSourceMapping",
        "lambda:getFunction",
        "lambda:getFunctionCodeSigningConfig",
        "lambda:getFunctionConcurrency",
        "lambda:getFunctionConfiguration",
```

```
        "lambda:getFunctionEventInvokeConfig",
        "lambda:getFunctionUrlConfig",
        "lambda:getLayerVersion",
        "lambda:getLayerVersionPolicy",
        "lambda:getPolicy",
        "lambda:getProvisionedConcurrencyConfig",
        "lambda:getRuntimeManagementConfig",
        "lambda:listAliases",
        "lambda:listCodeSigningConfigs",
        "lambda:listEventSourceMappings",
        "lambda:listFunctionEventInvokeConfigs",
        "lambda:listFunctionUrlConfigs",
        "lambda:listFunctions",
        "lambda:listFunctionsByCodeSigningConfig",
        "lambda:listLayerVersions",
        "lambda:listLayers",
        "lambda:listProvisionedConcurrencyConfigs",
        "lambda:listVersionsByFunction",
        "logs:describeExportTasks",
        "logs:describeLogGroups",
        "logs:describeLogStreams",
        "logs:describeMetricFilters",
        "logs:describeSubscriptionFilters",
        "medialive:listChannels",
        "medialive:listInputSecurityGroups",
        "medialive:listInputs",
        "mobiletargeting:getAdmChannel",
        "mobiletargeting:getApnsChannel",
        "mobiletargeting:getApnsSandboxChannel",
        "mobiletargeting:getApnsVoipChannel",
        "mobiletargeting:getApnsVoipSandboxChannel",
        "mobiletargeting:getApplicationSettings",
        "mobiletargeting:getApps",
        "mobiletargeting:getBaiduChannel",
        "mobiletargeting:getCampaign",
        "mobiletargeting:getCampaignActivities",
        "mobiletargeting:getCampaignVersions",
        "mobiletargeting:getCampaigns",
        "mobiletargeting:getEmailChannel",
        "mobiletargeting:getEventStream",
        "mobiletargeting:getExportJobs",
        "mobiletargeting:getGcmChannel",
        "mobiletargeting:getImportJobs",
        "mobiletargeting:getJourney",
```

```
        "mobiletargeting:getJourneyExecutionActivityMetrics",
        "mobiletargeting:getJourneyExecutionMetrics",
        "mobiletargeting:getJourneyRunExecutionActivityMetrics",
        "mobiletargeting:getJourneyRunExecutionMetrics",
        "mobiletargeting:getJourneyRuns",
        "mobiletargeting:getSegment",
        "mobiletargeting:getSegmentImportJobs",
        "mobiletargeting:getSegmentVersions",
        "mobiletargeting:getSegments",
        "mobiletargeting:getSmsChannel",
        "mobiletargeting:listJourneys",
        "pipes:listPipes",
        "polly:describeVoices",
        "polly:listLexicons",
        "quicksight:describeAccountCustomization",
        "quicksight:describeAccountSettings",
        "quicksight:describeAccountSubscription",
        "quicksight:describeAnalysis",
        "quicksight:describeAnalysisPermissions",
        "quicksight:describeDashboard",
        "quicksight:describeDashboardPermissions",
        "quicksight:describeDataSet",
        "quicksight:describeDataSetRefreshProperties",
        "quicksight:describeDataSource",
        "quicksight:describeFolder",
        "quicksight:describeFolderPermissions",
        "quicksight:describeFolderResolvedPermissions",
        "quicksight:describeGroup",
        "quicksight:describeGroupMembership",
        "quicksight:describeIAMPolicyAssignment",
        "quicksight:describeIngestion",
        "quicksight:describeIpRestriction",
        "quicksight:describeNamespace",
        "quicksight:describeRefreshSchedule",
        "quicksight:describeTemplate",
        "quicksight:describeTemplateAlias",
        "quicksight:describeTemplatePermissions",
        "quicksight:describeTheme",
        "quicksight:describeThemeAlias",
        "quicksight:describeThemePermissions",
        "quicksight:describeTopic",
        "quicksight:describeTopicRefresh",
        "quicksight:describeTopicRefreshSchedule",
        "quicksight:describeUser",
```

```
        "quicksight:describeVPCConnection",
        "quicksight:listAnalyses",
        "quicksight:listDashboardVersions",
        "quicksight:listDashboards",
        "quicksight:listDataSets",
        "quicksight:listDataSources",
        "quicksight:listFolderMembers",
        "quicksight:listFolders",
        "quicksight:listGroupMemberships",
        "quicksight:listGroups",
        "quicksight:listIAMPolicyAssignments",
        "quicksight:listIAMPolicyAssignmentsForUser",
        "quicksight:listIngestions",
        "quicksight:listNamespaces",
        "quicksight:listRefreshSchedules",
        "quicksight:listTemplateAliases",
        "quicksight:listTemplateVersions",
        "quicksight:listTemplates",
        "quicksight:listThemeAliases",
        "quicksight:listThemeVersions",
        "quicksight:listThemes",
        "quicksight:listTopicRefreshSchedules",
        "quicksight:listTopics",
        "quicksight:listUserGroups",
        "quicksight:listUsers",
        "quicksight:listVPCConnections",
        "quicksight:searchAnalyses",
        "quicksight:searchDashboards",
        "quicksight:searchDataSets",
        "quicksight:searchDataSources",
        "quicksight:searchFolders",
        "quicksight:searchGroups",
        "rds:describeAccountAttributes",
        "rds:describeBlueGreenDeployments",
        "rds:describeCertificates",
        "rds:describeDBClusterEndpoints",
        "rds:describeDBClusterParameterGroups",
        "rds:describeDBClusterParameters",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBClusters",
        "rds:describeDBEngineVersions",
        "rds:describeDBInstanceAutomatedBackups",
        "rds:describeDBInstances",
        "rds:describeDBLogFiles",
```

```
        "rds:describeDBParameterGroups",
        "rds:describeDBParameters",
        "rds:describeDBSecurityGroups",
        "rds:describeDBSnapshotAttributes",
        "rds:describeDBSnapshots",
        "rds:describeDBSubnetGroups",
        "rds:describeEngineDefaultClusterParameters",
        "rds:describeEngineDefaultParameters",
        "rds:describeEventCategories",
        "rds:describeEventSubscriptions",
        "rds:describeEvents",
        "rds:describeExportTasks",
        "rds:describeGlobalClusters",
        "rds:describeIntegrations",
        "rds:describeOptionGroupOptions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describePendingMaintenanceActions",
        "rds:describeReservedDBInstances",
        "rds:describeReservedDBInstancesOfferings",
        "rds:describeSourceRegions",
        "rds:describeValidDBInstanceModifications",
        "rds:listTagsForResource",
        "redshift-data:describeStatement",
        "redshift-data:listStatements",
        "redshift-serverless:getEndpointAccess",
        "redshift-serverless:getNamespace",
        "redshift-serverless:getRecoveryPoint",
        "redshift-serverless:getSnapshot",
        "redshift-serverless:getTableRestoreStatus",
        "redshift-serverless:getUsageLimit",
        "redshift-serverless:getWorkgroup",
        "redshift-serverless:listEndpointAccess",
        "redshift-serverless:listNamespaces",
        "redshift-serverless:listRecoveryPoints",
        "redshift-serverless:listSnapshots",
        "redshift-serverless:listTableRestoreStatus",
        "redshift-serverless:listUsageLimits",
        "redshift-serverless:listWorkgroups",
        "redshift:describeClusterParameterGroups",
        "redshift:describeClusterParameters",
        "redshift:describeClusterSecurityGroups",
        "redshift:describeClusterSnapshots",
        "redshift:describeClusterSubnetGroups",
```

```
        "redshift:describeClusterVersions",
        "redshift:describeClusters",
        "redshift:describeDataShares",
        "redshift:describeDataSharesForConsumer",
        "redshift:describeDataSharesForProducer",
        "redshift:describeDefaultClusterParameters",
        "redshift:describeEventCategories",
        "redshift:describeEventSubscriptions",
        "redshift:describeEvents",
        "redshift:describeHsmClientCertificates",
        "redshift:describeHsmConfigurations",
        "redshift:describeLoggingStatus",
        "redshift:describeOrderableClusterOptions",
        "redshift:describeReservedNodeOfferings",
        "redshift:describeReservedNodes",
        "redshift:describeResize",
        "redshift:describeSnapshotCopyGrants",
        "redshift:describeStorage",
        "redshift:describeTableRestoreStatus",
        "redshift:describeTags",
        "route53-recovery-cluster:getRoutingControlState",
        "route53-recovery-cluster:listRoutingControls",
        "route53-recovery-control-config:describeControlPanel",
        "route53-recovery-control-config:describeRoutingControl",
        "route53-recovery-control-config:describeSafetyRule",
        "route53-recovery-control-config:listControlPanels",
        "route53-recovery-control-config:listRoutingControls",
        "route53-recovery-control-config:listSafetyRules",
        "route53-recovery-readiness:getCell",
        "route53-recovery-readiness:getCellReadinessSummary",
        "route53-recovery-readiness:getReadinessCheck",
        "route53-recovery-readiness:getReadinessCheckResourceStatus",
        "route53-recovery-readiness:getReadinessCheckStatus",
        "route53-recovery-readiness:getRecoveryGroup",
        "route53-recovery-readiness:getRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:listCells",
        "route53-recovery-readiness:listReadinessChecks",
        "route53-recovery-readiness:listRecoveryGroups",
        "route53-recovery-readiness:listResourceSets",
        "route53:getAccountLimit",
        "route53:getChange",
        "route53:getCheckerIpRanges",
        "route53:getDNSSEC",
        "route53:getGeoLocation",
```

```
        "route53:getHealthCheck",
        "route53:getHealthCheckCount",
        "route53:getHealthCheckLastFailureReason",
        "route53:getHealthCheckStatus",
        "route53:getHostedZone",
        "route53:getHostedZoneCount",
        "route53:getHostedZoneLimit",
        "route53:getQueryLoggingConfig",
        "route53:getReusableDelegationSet",
        "route53:getTrafficPolicy",
        "route53:getTrafficPolicyInstance",
        "route53:getTrafficPolicyInstanceCount",
        "route53:listCidrBlocks",
        "route53:listCidrCollections",
        "route53:listCidrLocations",
        "route53:listGeoLocations",
        "route53:listHealthChecks",
        "route53:listHostedZones",
        "route53:listHostedZonesByName",
        "route53:listHostedZonesByVpc",
        "route53:listQueryLoggingConfigs",
        "route53:listResourceRecordSets",
        "route53:listReusableDelegationSets",
        "route53:listTrafficPolicies",
        "route53:listTrafficPolicyInstances",
        "route53:listTrafficPolicyInstancesByHostedZone",
        "route53:listTrafficPolicyInstancesByPolicy",
        "route53:listTrafficPolicyVersions",
        "route53:listVPCAssociationAuthorizations",
        "route53domains:checkDomainAvailability",
        "route53domains:getContactReachabilityStatus",
        "route53domains:getDomainDetail",
        "route53domains:getOperationDetail",
        "route53domains:listDomains",
        "route53domains:listOperations",
        "route53domains:listPrices",
        "route53domains:listTagsForDomain",
        "route53domains:viewBilling",
        "route53resolver:getFirewallConfig",
        "route53resolver:getFirewallDomainList",
        "route53resolver:getFirewallRuleGroup",
        "route53resolver:getFirewallRuleGroupAssociation",
        "route53resolver:getFirewallRuleGroupPolicy",
        "route53resolver:getOutpostResolver",
```

```
        "route53resolver:getResolverDnssecConfig",
        "route53resolver:getResolverQueryLogConfig",
        "route53resolver:getResolverQueryLogConfigAssociation",
        "route53resolver:getResolverQueryLogConfigPolicy",
        "route53resolver:getResolverRule",
        "route53resolver:getResolverRuleAssociation",
        "route53resolver:getResolverRulePolicy",
        "route53resolver:listFirewallConfigs",
        "route53resolver:listFirewallDomainLists",
        "route53resolver:listFirewallDomains",
        "route53resolver:listFirewallRuleGroupAssociations",
        "route53resolver:listFirewallRuleGroups",
        "route53resolver:listFirewallRules",
        "route53resolver:listOutpostResolvers",
        "route53resolver:listResolverConfigs",
        "route53resolver:listResolverDnssecConfigs",
        "route53resolver:listResolverEndpointIpAddresses",
        "route53resolver:listResolverEndpoints",
        "route53resolver:listResolverQueryLogConfigAssociations",
        "route53resolver:listResolverQueryLogConfigs",
        "route53resolver:listResolverRuleAssociations",
        "route53resolver:listResolverRules",
        "route53resolver:listTagsForResource",
        "s3:describeJob",
        "s3:describeMultiRegionAccessPointOperation",
        "s3:getAccelerateConfiguration",
        "s3:getAccessPoint",
        "s3:getAccessPointConfigurationForObjectLambda",
        "s3:getAccessPointForObjectLambda",
        "s3:getAccessPointPolicy",
        "s3:getAccessPointPolicyForObjectLambda",
        "s3:getAccessPointPolicyStatus",
        "s3:getAccessPointPolicyStatusForObjectLambda",
        "s3:getAccountPublicAccessBlock",
        "s3:getAnalyticsConfiguration",
        "s3:getBucketAcl",
        "s3:getBucketCORS",
        "s3:getBucketLocation",
        "s3:getBucketLogging",
        "s3:getBucketNotification",
        "s3:getBucketObjectLockConfiguration",
        "s3:getBucketOwnershipControls",
        "s3:getBucketPolicy",
        "s3:getBucketPolicyStatus",
```

```
        "s3:getBucketPublicAccessBlock",
        "s3:getBucketRequestPayment",
        "s3:getBucketVersioning",
        "s3:getBucketWebsite",
        "s3:getEncryptionConfiguration",
        "s3:getIntelligentTieringConfiguration",
        "s3:getInventoryConfiguration",
        "s3:getLifecycleConfiguration",
        "s3:getMetricsConfiguration",
        "s3:getMultiRegionAccessPoint",
        "s3:getMultiRegionAccessPointPolicy",
        "s3:getMultiRegionAccessPointPolicyStatus",
        "s3:getMultiRegionAccessPointRoutes",
        "s3:getObjectLegalHold",
        "s3:getObjectRetention",
        "s3:getReplicationConfiguration",
        "s3:getStorageLensConfiguration",
        "s3:listAccessPoints",
        "s3:listAccessPointsForObjectLambda",
        "s3:listAllMyBuckets",
        "s3:listBucket",
        "s3:listBucketMultipartUploads",
        "s3:listBucketVersions",
        "s3:listJobs",
        "s3:listMultiRegionAccessPoints",
        "s3:listMultipartUploadParts",
        "s3:listStorageLensConfigurations",
        "s3express:getBucketPolicy",
        "s3express:listAllMyDirectoryBuckets",
        "sagemaker:describeAction",
        "sagemaker:describeAlgorithm",
        "sagemaker:describeApp",
        "sagemaker:describeAppImageConfig",
        "sagemaker:describeArtifact",
        "sagemaker:describeAutoMLJob",
        "sagemaker:describeCluster",
        "sagemaker:describeClusterNode",
        "sagemaker:describeCodeRepository",
        "sagemaker:describeCompilationJob",
        "sagemaker:describeContext",
        "sagemaker:describeDataQualityJobDefinition",
        "sagemaker:describeDevice",
        "sagemaker:describeDeviceFleet",
        "sagemaker:describeDomain",
```

```
        "sagemaker:describeEdgeDeploymentPlan",
        "sagemaker:describeEdgePackagingJob",
        "sagemaker:describeEndpoint",
        "sagemaker:describeEndpointConfig",
        "sagemaker:describeExperiment",
        "sagemaker:describeFeatureGroup",
        "sagemaker:describeFeatureMetadata",
        "sagemaker:describeFlowDefinition",
        "sagemaker:describeHub",
        "sagemaker:describeHubContent",
        "sagemaker:describeHumanTaskUi",
        "sagemaker:describeHyperParameterTuningJob",
        "sagemaker:describeImage",
        "sagemaker:describeImageVersion",
        "sagemaker:describeInferenceComponent",
        "sagemaker:describeInferenceExperiment",
        "sagemaker:describeInferenceRecommendationsJob",
        "sagemaker:describeLabelingJob",
        "sagemaker:describeModel",
        "sagemaker:describeModelBiasJobDefinition",
        "sagemaker:describeModelCard",
        "sagemaker:describeModelCardExportJob",
        "sagemaker:describeModelExplainabilityJobDefinition",
        "sagemaker:describeModelPackage",
        "sagemaker:describeModelPackageGroup",
        "sagemaker:describeModelQualityJobDefinition",
        "sagemaker:describeMonitoringSchedule",
        "sagemaker:describeNotebookInstance",
        "sagemaker:describeNotebookInstanceLifecycleConfig",
        "sagemaker:describePipeline",
        "sagemaker:describePipelineDefinitionForExecution",
        "sagemaker:describePipelineExecution",
        "sagemaker:describeProcessingJob",
        "sagemaker:describeProject",
        "sagemaker:describeSpace",
        "sagemaker:describeStudioLifecycleConfig",
        "sagemaker:describeSubscribedWorkteam",
        "sagemaker:describeTrainingJob",
        "sagemaker:describeTransformJob",
        "sagemaker:describeTrial",
        "sagemaker:describeTrialComponent",
        "sagemaker:describeUserProfile",
        "sagemaker:describeWorkforce",
        "sagemaker:describeWorkteam",
```

```
        "sagemaker:getDeviceFleetReport",
        "sagemaker:getModelPackageGroupPolicy",
        "sagemaker:getSagemakerServicecatalogPortfolioStatus",
        "sagemaker:listActions",
        "sagemaker:listAlgorithms",
        "sagemaker:listAliases",
        "sagemaker:listAppImageConfigs",
        "sagemaker:listApps",
        "sagemaker:listArtifacts",
        "sagemaker:listAssociations",
        "sagemaker:listAutoMLJobs",
        "sagemaker:listCandidatesForAutoMLJob",
        "sagemaker:listClusterNodes",
        "sagemaker:listClusters",
        "sagemaker:listCodeRepositories",
        "sagemaker:listCompilationJobs",
        "sagemaker:listContexts",
        "sagemaker:listDataQualityJobDefinitions",
        "sagemaker:listDeviceFleets",
        "sagemaker:listDevices",
        "sagemaker:listDomains",
        "sagemaker:listEdgeDeploymentPlans",
        "sagemaker:listEdgePackagingJobs",
        "sagemaker:listEndpointConfigs",
        "sagemaker:listEndpoints",
        "sagemaker:listExperiments",
        "sagemaker:listFeatureGroups",
        "sagemaker:listFlowDefinitions",
        "sagemaker:listHubContentVersions",
        "sagemaker:listHubContents",
        "sagemaker:listHubs",
        "sagemaker:listHumanTaskUis",
        "sagemaker:listHyperParameterTuningJobs",
        "sagemaker:listImageVersions",
        "sagemaker:listImages",
        "sagemaker:listInferenceComponents",
        "sagemaker:listInferenceExperiments",
        "sagemaker:listInferenceRecommendationsJobSteps",
        "sagemaker:listInferenceRecommendationsJobs",
        "sagemaker:listLabelingJobs",
        "sagemaker:listLabelingJobsForWorkteam",
        "sagemaker:listLineageGroups",
        "sagemaker:listModelBiasJobDefinitions",
        "sagemaker:listModelCardExportJobs",
```

```
        "sagemaker:listModelCardVersions",
        "sagemaker:listModelCards",
        "sagemaker:listModelExplainabilityJobDefinitions",
        "sagemaker:listModelMetadata",
        "sagemaker:listModelPackageGroups",
        "sagemaker:listModelPackages",
        "sagemaker:listModelQualityJobDefinitions",
        "sagemaker:listModels",
        "sagemaker:listMonitoringAlertHistory",
        "sagemaker:listMonitoringAlerts",
        "sagemaker:listMonitoringExecutions",
        "sagemaker:listMonitoringSchedules",
        "sagemaker:listNotebookInstanceLifecycleConfigs",
        "sagemaker:listNotebookInstances",
        "sagemaker:listPipelineExecutionSteps",
        "sagemaker:listPipelineExecutions",
        "sagemaker:listPipelineParametersForExecution",
        "sagemaker:listPipelines",
        "sagemaker:listProcessingJobs",
        "sagemaker:listProjects",
        "sagemaker:listSpaces",
        "sagemaker:listStageDevices",
        "sagemaker:listStudioLifecycleConfigs",
        "sagemaker:listSubscribedWorkteams",
        "sagemaker:listTags",
        "sagemaker:listTrainingJobs",
        "sagemaker:listTrainingJobsForHyperParameterTuningJob",
        "sagemaker:listTransformJobs",
        "sagemaker:listTrialComponents",
        "sagemaker:listTrials",
        "sagemaker:listUserProfiles",
        "sagemaker:listWorkforces",
        "sagemaker:listWorkteams",
        "scheduler:listScheduleGroups",
        "scheduler:listSchedules",
        "servicequotas:listAWSDefaultServiceQuotas",
        "servicequotas:listServiceQuotas",
        "ses:describeActiveReceiptRuleSet",
        "ses:describeConfigurationSet",
        "ses:describeReceiptRule",
        "ses:describeReceiptRuleSet",
        "ses:getAccount",
        "ses:getAccountSendingEnabled",
        "ses:getBlacklistReports",
```

```
        "ses:getConfigurationSet",
        "ses:getConfigurationSetEventDestinations",
        "ses:getContactList",
        "ses:getDedicatedIp",
        "ses:getDedicatedIpPool",
        "ses:getDedicatedIps",
        "ses:getDeliverabilityDashboardOptions",
        "ses:getDeliverabilityTestReport",
        "ses:getDomainDeliverabilityCampaign",
        "ses:getDomainStatisticsReport",
        "ses:getEmailIdentity",
        "ses:getIdentityDkimAttributes",
        "ses:getIdentityMailFromDomainAttributes",
        "ses:getIdentityNotificationAttributes",
        "ses:getIdentityPolicies",
        "ses:getIdentityVerificationAttributes",
        "ses:getImportJob",
        "ses:getSendQuota",
        "ses:getSendStatistics",
        "ses:listConfigurationSets",
        "ses:listContactLists",
        "ses:listContacts",
        "ses:listCustomVerificationEmailTemplates",
        "ses:listDedicatedIpPools",
        "ses:listDeliverabilityTestReports",
        "ses:listDomainDeliverabilityCampaigns",
        "ses:listEmailIdentities",
        "ses:listEmailTemplates",
        "ses:listIdentities",
        "ses:listIdentityPolicies",
        "ses:listImportJobs",
        "ses:listReceiptFilters",
        "ses:listReceiptRuleSets",
        "ses:listRecommendations",
        "ses:listTagsForResource",
        "ses:listTemplates",
        "ses:listVerifiedEmailAddresses",
        "sns:checkIfPhoneNumberIsOptedOut",
        "sns:getDataProtectionPolicy",
        "sns:getEndpointAttributes",
        "sns:getPlatformApplicationAttributes",
        "sns:getSMSAttributes",
        "sns:getSMSSandboxAccountStatus",
        "sns:getSubscriptionAttributes",
```

```
        "sns:getTopicAttributes",
        "sns:listEndpointsByPlatformApplication",
        "sns:listOriginationNumbers",
        "sns:listPhoneNumbersOptedOut",
        "sns:listPlatformApplications",
        "sns:listSMSSandboxPhoneNumbers",
        "sns:listSubscriptions",
        "sns:listSubscriptionsByTopic",
        "sns:listTopics",
        "ssm-contacts:describeEngagement",
        "ssm-contacts:describePage",
        "ssm-contacts:getContact",
        "ssm-contacts:getContactChannel",
        "ssm-contacts:getContactPolicy",
        "ssm-contacts:getRotation",
        "ssm-contacts:getRotationOverride",
        "ssm-contacts:listContactChannels",
        "ssm-contacts:listContacts",
        "ssm-contacts:listEngagements",
        "ssm-contacts:listPageReceipts",
        "ssm-contacts:listPageResolutions",
        "ssm-contacts:listPagesByContact",
        "ssm-contacts:listPagesByEngagement",
        "ssm-contacts:listPreviewRotationShifts",
        "ssm-contacts:listRotationOverrides",
        "ssm-contacts:listRotationShifts",
        "ssm-contacts:listRotations",
        "ssm-incidents:getIncidentRecord",
        "ssm-incidents:getReplicationSet",
        "ssm-incidents:getResourcePolicies",
        "ssm-incidents:getResponsePlan",
        "ssm-incidents:getTimelineEvent",
        "ssm-incidents:listIncidentRecords",
        "ssm-incidents:listRelatedItems",
        "ssm-incidents:listReplicationSets",
        "ssm-incidents:listResponsePlans",
        "ssm-incidents:listTimelineEvents",
        "ssm-sap:getApplication",
        "ssm-sap:getComponent",
        "ssm-sap:getDatabase",
        "ssm-sap:getOperation",
        "ssm-sap:getResourcePermission",
        "ssm-sap:listApplications",
        "ssm-sap:listComponents",
```

```
        "ssm-sap:listDatabases",
        "ssm-sap:listOperations",
        "ssm:describeActivations",
        "ssm:describeAssociation",
        "ssm:describeAssociationExecutionTargets",
        "ssm:describeAssociationExecutions",
        "ssm:describeAutomationExecutions",
        "ssm:describeAutomationStepExecutions",
        "ssm:describeAvailablePatches",
        "ssm:describeDocument",
        "ssm:describeDocumentPermission",
        "ssm:describeEffectiveInstanceAssociations",
        "ssm:describeEffectivePatchesForPatchBaseline",
        "ssm:describeInstanceAssociationsStatus",
        "ssm:describeInstanceInformation",
        "ssm:describeInstancePatchStates",
        "ssm:describeInstancePatchStatesForPatchGroup",
        "ssm:describeInstancePatches",
        "ssm:describeInventoryDeletions",
        "ssm:describeMaintenanceWindowExecutionTaskInvocations",
        "ssm:describeMaintenanceWindowExecutionTasks",
        "ssm:describeMaintenanceWindowExecutions",
        "ssm:describeMaintenanceWindowSchedule",
        "ssm:describeMaintenanceWindowTargets",
        "ssm:describeMaintenanceWindowTasks",
        "ssm:describeMaintenanceWindows",
        "ssm:describeMaintenanceWindowsForTarget",
        "ssm:describeOpsItems",
        "ssm:describeParameters",
        "ssm:describePatchBaselines",
        "ssm:describePatchGroupState",
        "ssm:describePatchGroups",
        "ssm:describePatchProperties",
        "ssm:describeSessions",
        "ssm:getAutomationExecution",
        "ssm:getCalendarState",
        "ssm:getCommandInvocation",
        "ssm:getConnectionStatus",
        "ssm:getDefaultPatchBaseline",
        "ssm:getDeployablePatchSnapshotForInstance",
        "ssm:getInventorySchema",
        "ssm:getMaintenanceWindow",
        "ssm:getMaintenanceWindowExecution",
        "ssm:getMaintenanceWindowExecutionTask",
```

```
        "ssm:getMaintenanceWindowExecutionTaskInvocation",
        "ssm:getMaintenanceWindowTask",
        "ssm:getOpsItem",
        "ssm:getOpsMetadata",
        "ssm:getOpsSummary",
        "ssm:getPatchBaseline",
        "ssm:getPatchBaselineForPatchGroup",
        "ssm:getResourcePolicies",
        "ssm:getServiceSetting",
        "ssm:listAssociationVersions",
        "ssm:listAssociations",
        "ssm:listCommandInvocations",
        "ssm:listCommands",
        "ssm:listComplianceItems",
        "ssm:listComplianceSummaries",
        "ssm:listDocumentMetadataHistory",
        "ssm:listDocumentVersions",
        "ssm:listDocuments",
        "ssm:listOpsItemEvents",
        "ssm:listOpsItemRelatedItems",
        "ssm:listOpsMetadata",
        "ssm:listResourceComplianceSummaries",
        "ssm:listResourceDataSync",
        "ssm:listTagsForResource",
        "swf:describeActivityType",
        "swf:describeDomain",
        "swf:describeWorkflowExecution",
        "swf:describeWorkflowType",
        "swf:getWorkflowExecutionHistory",
        "swf:listActivityTypes",
        "swf:listClosedWorkflowExecutions",
        "swf:listDomains",
        "swf:listOpenWorkflowExecutions",
        "swf:listWorkflowTypes",
        "vpc-lattice:getAccessLogSubscription",
        "vpc-lattice:getAuthPolicy",
        "vpc-lattice:getListener",
        "vpc-lattice:getResourcePolicy",
        "vpc-lattice:getRule",
        "vpc-lattice:getService",
        "vpc-lattice:getServiceNetwork",
        "vpc-lattice:getServiceNetworkServiceAssociation",
        "vpc-lattice:getServiceNetworkVpcAssociation",
        "vpc-lattice:getTargetGroup",
```

```
        "vpc-lattice:listAccessLogSubscriptions",
        "vpc-lattice:listListeners",
        "vpc-lattice:listRules",
        "vpc-lattice:listServiceNetworkServiceAssociations",
        "vpc-lattice:listServiceNetworkVpcAssociations",
        "vpc-lattice:listServiceNetworks",
        "vpc-lattice:listServices",
        "vpc-lattice:listTargetGroups",
        "vpc-lattice:listTargets",
        "waf-regional:getByteMatchSet",
        "waf-regional:getChangeTokenStatus",
        "waf-regional:getGeoMatchSet",
        "waf-regional:getIPSet",
        "waf-regional:getLoggingConfiguration",
        "waf-regional:getRateBasedRule",
        "waf-regional:getRegexMatchSet",
        "waf-regional:getRegexPatternSet",
        "waf-regional:getRule",
        "waf-regional:getRuleGroup",
        "waf-regional:getSqlInjectionMatchSet",
        "waf-regional:getWebACL",
        "waf-regional:getWebACLForResource",
        "waf-regional:listActivatedRulesInRuleGroup",
        "waf-regional:listByteMatchSets",
        "waf-regional:listGeoMatchSets",
        "waf-regional:listIPSets",
        "waf-regional:listLoggingConfigurations",
        "waf-regional:listRateBasedRules",
        "waf-regional:listRegexMatchSets",
        "waf-regional:listRegexPatternSets",
        "waf-regional:listResourcesForWebACL",
        "waf-regional:listRuleGroups",
        "waf-regional:listRules",
        "waf-regional:listSqlInjectionMatchSets",
        "waf-regional:listWebACLs",
        "waf:getByteMatchSet",
        "waf:getChangeTokenStatus",
        "waf:getGeoMatchSet",
        "waf:getIPSet",
        "waf:getLoggingConfiguration",
        "waf:getRateBasedRule",
        "waf:getRegexMatchSet",
        "waf:getRegexPatternSet",
        "waf:getRule",
```

```
        "waf:getRuleGroup",
        "waf:getSampledRequests",
        "waf:getSizeConstraintSet",
        "waf:getSqlInjectionMatchSet",
        "waf:getWebACL",
        "waf:getXssMatchSet",
        "waf:listActivatedRulesInRuleGroup",
        "waf:listByteMatchSets",
        "waf:listGeoMatchSets",
        "waf:listIPSets",
        "waf:listLoggingConfigurations",
        "waf:listRateBasedRules",
        "waf:listRegexMatchSets",
        "waf:listRegexPatternSets",
        "waf:listRuleGroups",
        "waf:listRules",
        "waf:listSizeConstraintSets",
        "waf:listSqlInjectionMatchSets",
        "waf:listWebACLs",
        "waf:listXssMatchSets",
        "wafv2:checkCapacity",
        "wafv2:describeManagedRuleGroup",
        "wafv2:getIPSet",
        "wafv2:getLoggingConfiguration",
        "wafv2:getPermissionPolicy",
        "wafv2:getRateBasedStatementManagedKeys",
        "wafv2:getRegexPatternSet",
        "wafv2:getRuleGroup",
        "wafv2:getSampledRequests",
        "wafv2:getWebACL",
        "wafv2:getWebACLForResource",
        "wafv2:listAvailableManagedRuleGroups",
        "wafv2:listIPSets",
        "wafv2:listLoggingConfigurations",
        "wafv2:listRegexPatternSets",
        "wafv2:listResourcesForWebACL",
        "wafv2:listRuleGroups",
        "wafv2:listTagsForResource",
        "wafv2:listWebACLs",
        "workspaces-web:getBrowserSettings",
        "workspaces-web:getIdentityProvider",
        "workspaces-web:getNetworkSettings",
        "workspaces-web:getPortal",
        "workspaces-web:getPortalServiceProviderMetadata",
```

```
        "workspaces-web:getTrustStoreCertificate",
        "workspaces-web:getUserSettings",
        "workspaces-web:listBrowserSettings",
        "workspaces-web:listIdentityProviders",
        "workspaces-web:listNetworkSettings",
        "workspaces-web:listPortals",
        "workspaces-web:listTagsForResource",
        "workspaces-web:listTrustStoreCertificates",
        "workspaces-web:listTrustStores",
        "workspaces-web:listUserSettings",
        "workspaces:describeAccount",
        "workspaces:describeAccountModifications",
        "workspaces:describeApplicationAssociations",
        "workspaces:describeIpGroups",
        "workspaces:describeTags",
        "workspaces:describeWorkspaceAssociations",
        "workspaces:describeWorkspaceBundles",
        "workspaces:describeWorkspaceDirectories",
        "workspaces:describeWorkspaceImages",
        "workspaces:describeWorkspaces",
        "workspaces:describeWorkspacesConnectionStatus"
      ],
      "Resource" : [
        "*"
      ]
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPartnerProServeToolsFullAccess

Deskripsi: Menyediakan akses penuh ke ProServe alat.

`AWSPartnerProServeToolsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPartnerProServeToolsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Maret 2026, 21:57 UTC
- Waktu teredit: 23 Maret 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerProServeToolsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowProServeToolsFullAccess",
      "Effect" : "Allow",
      "Action" : "partnercentral-account-management:AccessProServeTools",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "partnercentral-account-management:ProServeRole" : [
            "AssessmentIndividualContributor",
            "AssessmentOrganizationReader",
            "AssessmentOrganizationContributor",
            "OrganizationAdmin"
          ]
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPartnerProServeToolsIndividualContributor

Deskripsi: Menyediakan akses untuk membuat dan mengelola penilaian sendiri di ProServe alat.

`AWSPartnerProServeToolsIndividualContributor`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPartnerProServeToolsIndividualContributor` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Maret 2026, 21:57 UTC
- Waktu teredit: 23 Maret 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerProServeToolsIndividualContributor`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowProServeToolsIndividualContributorAccess",
      "Effect" : "Allow",
      "Action" : "partnercentral-account-management:AccessProServeTools",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "partnercentral-account-management:ProServeRole" : [
            "AssessmentIndividualContributor"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPartnerProServeToolsOrganizationReaderIndividualContributor

Deskripsi: Menyediakan akses baca ke penilaian organisasi dengan kemampuan untuk mengelola penilaian sendiri.

`AWSPartnerProServeToolsOrganizationReaderIndividualContributor`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPartnerProServeToolsOrganizationReaderIndividualContributor` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Maret 2026, 22:12 UTC
- Waktu teredit: 23 Maret 2026, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerProServeToolsOrganizationReaderIndividualContributor`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowProServeToolsOrgReaderIndividualContributorAccess",
      "Effect" : "Allow",
      "Action" : "partnercentral-account-management:AccessProServeTools",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "partnercentral-account-management:ProServeRole" : [
            "AssessmentOrganizationReader",
            "AssessmentIndividualContributor"
          ]
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPCSComputeNodePolicy

Deskripsi: Memberikan izin ke node komputasi AWS PCS untuk terhubung ke cluster AWS PCS.

`AWSPCSComputeNodePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPCSComputeNodePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Juni 2025, 18:07 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPCSComputeNodePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pcs:RegisterComputeNodeGroupInstance"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPCSServiceRolePolicy

Deskripsi: Memberikan izin kepada PCS untuk mengelola sumber daya atas nama Anda.

`AWSPCSServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 27 Agustus 2024, 16:01 UTC
- Waktu teredit: 30 September 2026, 18:07 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPCSServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsToCreatePCSNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToCreatePCSNetworkInterfacesInSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "PermissionsToManagePCSNetworkInterfaces",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToDescribePCSResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeImages",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PermissionsToCreatePCSLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSPCSManaged" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "PermissionsToManagePCSLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToTerminatePCSManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToPassRoleToEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*/AWSPCS*",
        "arn:aws:iam::*:role/AWSPCS*",
        "arn:aws:iam::*:role/aws-pcs/*",
        "arn:aws:iam::*:role/*/aws-pcs/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsToControlClusterInstanceAttributes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:resource-groups:*:*:group/*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:spot-instances-request/*",
        "arn:aws:ec2:*:*:secondary-interface/*",
        "arn:aws:ec2:*:*:secondary-subnet/*"
      ]
    },
    {
      "Sid" : "PermissionsToProvisionClusterInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSPCSManaged" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "PermissionsToTagPCSResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateLaunchTemplate",
            "CreateFleet",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsToPublishMetrics",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/PCS"
        }
      }
    },
    {
      "Sid" : "PermissionsToManageSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:pcs!*",
      "Condition" : {
```

```
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "pcs",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPriceListServiceFullAccess

Deskripsi: Menyediakan akses penuh ke Layanan Daftar AWS Harga.

`AWSPriceListServiceFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPriceListServiceFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 November 2017, 00:36 UTC
- Waktu teredit: 02 Juli 2024, 13:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSPriceListServiceFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pricing:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPrivateCAAuditor

Deskripsi: Menyediakan akses auditor ke Otor AWS itas Sertifikat Swasta

`AWSPrivateCAAuditor`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPrivateCAAuditor` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Februari 2023, 18:33 UTC
- Waktu teredit: 14 Februari 2023, 18:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAAuditor`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:CreateCertificateAuthorityAuditReport",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:GetPolicy",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPrivateCAConnectorForKubernetesPolicy

Deskripsi: Memberikan izin penting untuk Konektor CA AWS Pribadi untuk Kubernetes.

`AWSPrivateCAConnectorForKubernetesPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPrivateCAConnectorForKubernetesPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Mei 2025, 19:22 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAConnectorForKubernetesPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificate",
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPrivateCAFullAccess

Deskripsi: Menyediakan akses penuh ke Otor AWS itas Sertifikat Pribadi

`AWSPrivateCAFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPrivateCAFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Februari 2023, 18:20 UTC

- Waktu teredit: 14 Februari 2023, 18:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPrivateCAPrivilegedUser

Deskripsi: Menyediakan akses pengguna sertifikat istimewa ke Otor AWS itas Sertifikat Pribadi

`AWSPrivateCAPrivilegedUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPrivateCAPrivilegedUser` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Februari 2023, 18:26 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAPrivilegedUser`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
```

```
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPrivateCAReadOnly

Deskripsi: Menyediakan akses baca saja ke Otor AWS itas Sertifikat Pribadi

`AWSPrivateCAReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPrivateCAReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Februari 2023, 18:30 UTC
- Waktu teredit: 14 Februari 2023, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:DescribeCertificateAuthorityAuditReport",
      "acm-pca:ListCertificateAuthorities",
      "acm-pca:GetCertificateAuthorityCsr",
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:GetCertificate",
      "acm-pca:GetPolicy",
      "acm-pca:ListPermissions",
      "acm-pca:ListTags"
    ],
    "Resource" : "*"
  }
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPrivateCAUser

Deskripsi: Menyediakan akses pengguna sertifikat ke Otor AWS itas Sertifikat Pribadi

`AWSPrivateCAUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPrivateCAUser` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Februari 2023, 18:16 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAUser`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPrivateMarketplaceAdminFullAccess

Deskripsi: Menyediakan akses penuh ke semua tindakan administratif untuk AWS Pasar Pribadi.

`AWSPrivateMarketplaceAdminFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPrivateMarketplaceAdminFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2018, 16:32 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrivateMarketplaceGetRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*AWSServiceRoleForPrivateMarketplaceAdmin"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceCreateSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/private-
marketplace.marketplace.amazonaws.com/AWSServiceRoleForPrivateMarketplaceAdmin"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "private-marketplace.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PrivateMarketplaceManageDelegatedAdministratorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "private-
marketplace.marketplace.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "PrivateMarketplaceEnableServiceAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "private-
marketplace.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PrivateMarketplaceRequestPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:AssociateProductsWithPrivateMarketplace",
        "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceCatalogAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:CancelChangeSet"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "PrivateMarketplaceCatalogTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Sid" : "PrivateMarketplaceOrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPrivateMarketplaceRequests

Deskripsi: Menyediakan akses untuk membuat permintaan di Pasar AWS Pribadi.

`AWSPrivateMarketplaceRequests`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPrivateMarketplaceRequests` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Oktober 2019, 21:44 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceRequests`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LegacyPrivateMarketplaceRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceManageRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
```

```
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProductProcurementRequest/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : [
            "CreateProductProcurementRequest",
            "CancelProductProcurementRequest"
          ]
        }
      }
    },
    {
      "Sid" : "PrivateMarketplaceReadRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProductProcurementRequest/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceListRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceReadChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ]
    },
    {
```

```
      "Sid" : "PrivateMarketplaceTaggingRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProductProcurementRequest/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPrivateNetworksServiceRolePolicy

Deskripsi: Men AWS gizinkan Layanan Jaringan Pribadi untuk mengelola sumber daya atas nama pelanggan.

`AWSPrivateNetworksServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 16 Desember 2021, 23:17 UTC
- Waktu teredit: 16 Desember 2021, 23:17 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Private5G"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSProtonCodeBuildProvisioningBasicAccess

Deskripsi: Iz CodeBuild in perlu menjalankan build untuk AWS Proton Pro CodeBuild visioning.

`AWSProtonCodeBuildProvisioningBasicAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSProtonCodeBuildProvisioningBasicAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 November 2022, 21:04 UTC
- Waktu teredit: 09 November 2022, 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/AWSProton-*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "proton:NotifyResourceDeploymentStatusChange",
      "Resource" : "arn:aws:proton:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSProtonCodeBuildProvisioningServiceRolePolicy

Deskripsi: Men AWS gizinkan Proton mengelola penyediaan sumber daya Proton menggunakan CodeBuild dan AWS layanan lain atas nama Anda.

`AWSProtonCodeBuildProvisioningServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 09 November 2022, 21:32 UTC
- Waktu teredit: 17 Mei 2023, 16:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ListStackResources"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/AWSProton-CodeBuild-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:UpdateProject",
        "codebuild:StartBuild",
        "codebuild:StopBuild",
        "codebuild:RetryBuild",
        "codebuild:BatchGetBuilds",
        "codebuild:BatchGetProjects"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/AWSProton*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "codebuild.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSProtonDeveloperAccess

Deskripsi: Menyediakan akses AWS ke API Proton dan Konsol Manajemen, tetapi tidak mengizinkan administrasi templat atau lingkungan Proton.

`AWSProtonDeveloperAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSProtonDeveloperAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Februari 2021, 19:02 UTC
- Waktu teredit: 06 Juni 2024, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonDeveloperAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProtonPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineExecution",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codestar-connections:ListConnections",
        "codestar-connections:UseConnection",
        "proton:CancelServiceInstanceDeployment",
        "proton:CancelServicePipelineDeployment",
        "proton:CreateService",
        "proton:DeleteService",
        "proton:GetAccountRoles",
        "proton:GetAccountSettings",
        "proton:GetEnvironment",
        "proton:GetEnvironmentAccountConnection",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateMajorVersion",
        "proton:GetEnvironmentTemplateMinorVersion",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetRepository",
        "proton:GetRepositorySyncStatus",
        "proton:GetResourcesSummary",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
```

```
        "proton:GetServiceTemplateMajorVersion",
        "proton:GetServiceTemplateMinorVersion",
        "proton:GetServiceTemplateVersion",
        "proton:GetTemplateSyncConfig",
        "proton:GetTemplateSyncStatus",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentOutputs",
        "proton:ListEnvironmentProvisionedResources",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplateMajorVersions",
        "proton:ListEnvironmentTemplateMinorVersions",
        "proton:ListEnvironmentTemplates",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListRepositories",
        "proton:ListRepositorySyncDefinitions",
        "proton:ListServiceInstanceOutputs",
        "proton:ListServiceInstanceProvisionedResources",
        "proton:ListServiceInstances",
        "proton:ListServicePipelineOutputs",
        "proton:ListServicePipelineProvisionedResources",
        "proton:ListServices",
        "proton:ListServiceTemplateMajorVersions",
        "proton:ListServiceTemplateMinorVersions",
        "proton:ListServiceTemplates",
        "proton:ListServiceTemplateVersions",
        "proton:ListTagsForResource",
        "proton:UpdateService",
        "proton:UpdateServiceInstance",
        "proton:UpdateServicePipeline",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsPermissions",
      "Effect" : "Allow",
      "Action" : "codestar-connections:PassConnection",
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "codestar-connections:PassedToService" : "proton.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeConnectionsPermissions",
      "Effect" : "Allow",
      "Action" : "codeconnections:PassConnection",
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codeconnections:PassedToService" : "proton.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSProtonFullAccess

Deskripsi: Menyediakan akses penuh ke AWS API Proton dan Konsol Manajemen. Selain izin ini, akses ke Amazon S3 juga diperlukan untuk mendaftarkan bundel template dari bucket S3 Anda, serta akses ke Amazon IAM untuk membuat dan mengelola peran layanan untuk Proton.

`AWSProtonFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSProtonFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Februari 2021, 19:07 UTC
- Waktu teredit: 06 Juni 2024, 18:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProtonPermissions",
      "Effect" : "Allow",
      "Action" : [
        "proton:*",
        "codestar-connections:ListConnections",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "kms:ViaService" : "proton.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "proton.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sync.proton.amazonaws.com/
AWSServiceRoleForProtonSync",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "sync.proton.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeStarConnectionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:PassConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "proton.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "CodeConnectionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:PassConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codeconnections:PassedToService" : "proton.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSProtonReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke AWS API Proton dan Konsol Manajemen.

`AWSProtonReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSProtonReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 17 Februari 2021, 19:09 UTC
- Waktu teredit: 18 November 2022 18.28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "proton:GetAccountRoles",
        "proton:GetAccountSettings",
        "proton:GetEnvironment",
        "proton:GetEnvironmentAccountConnection",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateMajorVersion",
        "proton:GetEnvironmentTemplateMinorVersion",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetRepository",
        "proton:GetRepositorySyncStatus",
        "proton:GetResourcesSummary",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateMajorVersion",
        "proton:GetServiceTemplateMinorVersion",
```

```
        "proton:GetServiceTemplateVersion",
        "proton:GetTemplateSyncConfig",
        "proton:GetTemplateSyncStatus",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentOutputs",
        "proton:ListEnvironmentProvisionedResources",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplateMajorVersions",
        "proton:ListEnvironmentTemplateMinorVersions",
        "proton:ListEnvironmentTemplates",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListRepositories",
        "proton:ListRepositorySyncDefinitions",
        "proton:ListServiceInstanceOutputs",
        "proton:ListServiceInstanceProvisionedResources",
        "proton:ListServiceInstances",
        "proton:ListServicePipelineOutputs",
        "proton:ListServicePipelineProvisionedResources",
        "proton:ListServices",
        "proton:ListServiceTemplateMajorVersions",
        "proton:ListServiceTemplateMinorVersions",
        "proton:ListServiceTemplates",
        "proton:ListServiceTemplateVersions",
        "proton:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSProtonServiceGitSyncServiceRolePolicy

Deskripsi: Kebijakan yang memungkinkan AWS Proton untuk menyinkronkan definisi layanan, lingkungan, dan komponen Anda dari repositori git Anda ke AWS Proton.

`AWSProtonServiceGitSyncServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 04 April 2023, 15:55 UTC
- Waktu teredit: 04 April 2023, 15:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProtonServiceSync",
      "Effect" : "Allow",
      "Action" : [
        "proton:GetService",
```

```
        "proton:UpdateService",
        "proton:UpdateServicePipeline",
        "proton:GetServiceInstance",
        "proton:CreateServiceInstance",
        "proton:UpdateServiceInstance",
        "proton:ListServiceInstances",
        "proton:GetComponent",
        "proton:CreateComponent",
        "proton:ListComponents",
        "proton:UpdateComponent",
        "proton:GetEnvironment",
        "proton:CreateEnvironment",
        "proton:ListEnvironments",
        "proton:UpdateEnvironment"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSProtonSyncServiceRolePolicy

Deskripsi: Kebijakan yang memungkinkan AWS Proton untuk menyinkronkan konten repositori git Anda ke Proton atau menyinkronkan konten Proton ke repositori git Anda.

`AWSProtonSyncServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran

- Waktu pembuatan: 23 November 2021, 21:14 UTC
- Waktu teredit: 05 Mei 2024, 01:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SyncToProton",
      "Effect" : "Allow",
      "Action" : [
        "proton:UpdateServiceTemplateVersion",
        "proton:UpdateServiceTemplate",
        "proton:UpdateEnvironmentTemplateVersion",
        "proton:UpdateEnvironmentTemplate",
        "proton:GetServiceTemplateVersion",
        "proton:GetServiceTemplate",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetEnvironmentTemplate",
        "proton:DeleteServiceTemplateVersion",
        "proton:DeleteEnvironmentTemplateVersion",
        "proton:CreateServiceTemplateVersion",
        "proton:CreateServiceTemplate",
        "proton:CreateEnvironmentTemplateVersion",
        "proton:CreateEnvironmentTemplate",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListServiceTemplateVersions",
        "proton:CreateEnvironmentTemplateMajorVersion",
        "proton:CreateServiceTemplateMajorVersion"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSPurchaseOrdersServiceRolePolicy

Deskripsi: Memberikan izin untuk melihat dan mengubah pesanan pembelian di konsol penagihan

`AWSPurchaseOrdersServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPurchaseOrdersServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Mei 2020, 18:15 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetContactInformation",
        "aws-portal:*Billing",
        "consolidatedbilling:GetAccountBillingRole",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceUnits",
        "payments:GetPaymentInstrument",
        "payments:ListPaymentPreferences",
        "purchase-orders:AddPurchaseOrder",
        "purchase-orders:DeletePurchaseOrder",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "purchase-orders:ModifyPurchaseOrders",
        "purchase-orders:TagResource",
        "purchase-orders:UntagResource",
        "purchase-orders:UpdatePurchaseOrder",
        "purchase-orders:UpdatePurchaseOrderStatus",
        "purchase-orders:ViewPurchaseOrders",
        "tax:ListTaxRegistrations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSetupCFGCPacksPermissionsBoundary

Deskripsi: AWSQuickSetupCFGCPacksPermissionsBoundary Kebijakan menentukan daftar izin yang diizinkan dalam peran IAM yang dibuat oleh Pengaturan Cepat. Penyiapan Cepat menggunakan peran yang dibuat dengan kebijakan ini untuk menerapkan paket kesesuaian Con AWS fig.

`AWSQuickSetupCFGCPacksPermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupCFGCPacksPermissionsBoundary` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juni 2024, 09:52 UTC
- Waktu teredit: 26 Juni 2024, 09:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupCFGCPacksPermissionsBoundary`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConfigurationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-CFGCPacks*"
      ]
    },
    {
      "Sid" : "ConfigurationRolePassToSSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-CFGCPacks*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PutCPackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConformancePack"
      ],
      "Resource" : [
        "arn:aws:config:*:*:conformance-pack/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeCPacksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConformancePackStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConformancePacksSLRCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config-conforms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SystemsManagerSLRCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "EnableExplorerReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ServiceSettingsForExplorerUpdatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSetupDeploymentRolePolicy

Deskripsi: Menyediakan izin untuk Pengaturan Cepat Manajer AWS Sistem untuk menerapkan beberapa jenis konfigurasi. Jenis konfigurasi ini membuat peran dan otomatisasi IAM yang mengonfigurasi layanan dan fitur Amazon Web Services yang sering digunakan dengan praktik terbaik yang direkomendasikan.

`AWSQuickSetupDeploymentRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupDeploymentRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juni 2024, 09:55 UTC
- Waktu teredit: 07 September 2026, 15:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupDeploymentRolePolicy`

Versi kebijakan

Versi kebijakan: v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CfnRead",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
```

```
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*"
      ]
    },
    {
      "Sid" : "CfnTagOnMutate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack",
            "UpdateStack",
            "CreateChangeSet",
            "ExecuteChangeSet"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "RGroupsGet",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CPacksRead",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConformancePacks",
        "config:DescribeConformancePackStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OpsPacksManage",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConformancePack",
        "config:DeleteConformancePack"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : "arn:aws:config:*:*:conformance-pack/AWS-QuickSetup-*"
    },
    {
      "Sid" : "QSDocsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument",
        "ssm:UpdateDocument",
```

```
        "ssm:UpdateDocumentDefaultVersion",
        "ssm:DeleteDocument",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "ssm:ListTagsForResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPack-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPackInstance-*"
      ]
    },
    {
      "Sid" : "QSDocsRead",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPack*",
        "arn:aws:ssm:*::document/AWSConformancePacks-*",
        "arn:aws:ssm:*::document/AWSEC2-UpdateLaunchAgent",
        "arn:aws:ssm:*::document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*::document/AWS-RunPatchBaselineAssociation",
        "arn:aws:ssm:*::document/AWS-UpdateSSMAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableConfigRecording",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
        "arn:aws:ssm:*::document/AmazonCloudWatch-ManageAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-InstallAndManageCloudWatchAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ConfigureDevOpsGuru",
        "arn:aws:ssm:*::document/AWSQuickSetupType-DeployConformancePack",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ApplyInstanceState"
      ]
```

```
    },
    {
      "Sid" : "QSAssociationsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPack*",
        "arn:aws:ssm:*::document/AWSEC2-UpdateLaunchAgent",
        "arn:aws:ssm:*::document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*::document/AWS-RunPatchBaselineAssociation",
        "arn:aws:ssm:*::document/AWS-UpdateSSMAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableConfigRecording",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ApplyInstanceState",
        "arn:aws:ssm:*::document/AmazonCloudWatch-ManageAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-InstallAndManageCloudWatchAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ConfigureDevOpsGuru",
        "arn:aws:ssm:*::document/AWSQuickSetupType-DeployConformancePack",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "EventRulesManage",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
```

```
        "events:PutRule",
        "events:DeleteRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/*QuickSetup-*"
      ]
    },
    {
      "Sid" : "CPacksSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config-conforms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SSMSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "QSConfigRoleManage",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole",
        "iam:UpdateRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags",
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ]
    },
    {
      "Sid" : "QSConfigRolePass",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com",
            "events.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "DocDescribe",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LegacyDocClean",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteDocument"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
    {
      "Sid" : "LegacyIAMClean",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/*QuickSetup-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
    {
      "Sid" : "QSConfigRoleBounded",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRolePolicy",
        "iam:PutRolePolicy",
        "iam:PutRolePermissionsBoundary"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : [
            "arn:aws:iam::aws:policy/AWSQuickSetupCFGCPacksPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupCFGRecordingPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupDevOpsGuruPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupDistributorPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupSchedulerPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupSSMHostMgmtPermissionsBoundary"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ]
    },
    {
      "Sid" : "QSConfigRoleManagedPolicies",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy",
            "arn:aws:iam::aws:policy/
AWSSystemsManagerEnableConfigRecordingExecutionPolicy",
            "arn:aws:iam::aws:policy/
AWSQuickSetupManagedInstanceProfileExecutionPolicy",
            "arn:aws:iam::aws:policy/AWSQuickSetupStartStopInstancesExecutionPolicy",
```

```
            "arn:aws:iam::aws:policy/AWSQuickSetupStartSSMAssociationsExecutionPolicy"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSetupDevOpsGuruPermissionsBoundary

Deskripsi: AWSQuickSetupDevOpsGuruPermissionsBoundary Kebijakan menentukan daftar izin yang diizinkan dalam peran IAM yang dibuat oleh Pengaturan Cepat. Penyiapan Cepat menggunakan peran yang dibuat dengan kebijakan ini untuk mengaktifkan dan mengonfigurasi Amazon DevOps Guru. Kebijakan ini juga memberikan izin untuk mengaktifkan System Manager Explorer.

`AWSQuickSetupDevOpsGuruPermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupDevOpsGuruPermissionsBoundary` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juni 2024, 09:44 UTC
- Waktu teredit: 26 Juni 2024, 09:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupDevOpsGuruPermissionsBoundary`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateDevOpsGuruSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "devops-guru.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudformationReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DevOpsGuruNotificationChannelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:AddNotificationChannel"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:DevOpsGuru-Default-Topic",
        "arn:aws:devops-guru:*:*:/channels"
      ]
    },
    {
      "Sid" : "DevOpsGuruConfigurationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:UpdateResourceCollection",
        "devops-guru:UpdateServiceIntegration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSReadOnlyPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DevOpsGuruDefaultSNSTopicConfigurationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:AddPermission",
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:Publish",
        "sns:SetTopicAttributes",
        "sns:RemovePermission"
      ],
      "Resource" : "arn:aws:sns:*:*:DevOpsGuru-Default-Topic"
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
```

```
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSetupDistributorPermissionsBoundary

Deskripsi QuickSetup : membuat peran IAM yang memungkinkannya untuk mengonfigurasi fitur Distributor Manajer Sistem atas nama Anda, dan menggunakan kebijakan ini saat membuat peran tersebut untuk menentukan batas izin mereka.

`AWSQuickSetupDistributorPermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupDistributorPermissionsBoundary` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juni 2024, 09:50 UTC
- Waktu teredit: 26 Juni 2024, 09:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupDistributorPermissionsBoundary`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DistributorAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-*"
      ]
    },
    {
      "Sid" : "DistributorAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRoleManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:UpdateRole",
```

```
        "iam:GetRole"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-
*"
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceRolePassToEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToSSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
```

```
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "InstanceManagementPoliciesAttachPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils",
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore"
          ]
        },
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-
*"
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "DefaultInstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
```

```
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceProfileDisassociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "ConfigurationAutomationsStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-Distributor-*",
        "arn:aws:ssm:*:*:automation-definition/UpdateCloudWatchDocument-Distributor-*",
        "arn:aws:ssm:*:*:automation-definition/AWS-ConfigureAWSPackage*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*"
      ]
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingHostManagementBySSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListTagsForResource",
        "ssm:GetAutomationExecution",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSetupEnableAREXExecutionPolicy

Deskripsi: Kebijakan ini memberikan izin yang memungkinkan Manajer Sistem menjalankan runbook AWSQuickSetupType-EnableAREX Otomasi, yang mengaktifkan AWS Resource Explorer untuk digunakan dengan Manajer Sistem.

`AWSQuickSetupEnableAREXExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupEnableAREXExecutionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 November 2024, 22:45 UTC
- Waktu teredit: 15 November 2024, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupEnableAREXExecutionPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadActions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
```

```
        "resource-explorer-2:ListViews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowUpdateExistingIndexAndAssociateDefaultView",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:AssociateDefaultView"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateViewAndIndex",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:CreateView",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:TagResource"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*:*:view/all-resources/*",
        "arn:aws:resource-explorer-2:*:*:index/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Type" : "QuickSetup",
          "aws:ResourceTag/Type" : "QuickSetup"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "Type"
        }
      }
    },
    {
      "Sid" : "AllowCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
```

```
            "resource-explorer-2.amazonaws.com"
          ]
        }
      },
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSetupEnableDHMCExecutionPolicy

Deskripsi: Kebijakan ini memberikan izin yang memungkinkan kepala sekolah menjalankan runbook AWSQuickSetupType-EnableDHMC Otomasi, yang mengaktifkan Konfigurasi Manajemen Host Default.

`AWSQuickSetupEnableDHMCExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupEnableDHMCExecutionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 November 2024, 21:27 UTC
- Waktu teredit: 15 November 2024, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupEnableDHMCExecutionPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-DefaultEC2MgmtRole-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-DefaultEC2MgmtRole-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-DefaultEC2MgmtRole-*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AmazonSSMManagedEC2InstanceDefaultPolicy"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetServiceSetting",
        "ssm:UpdateServiceSetting"
      ],
      "Resource" : "arn:aws:ssm:*:*:servicesetting/ssm/managed-instance/default-ec2-
instance-management-role"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSetupJITNADeploymentRolePolicy

Deskripsi: Kebijakan ini memungkinkan Pengaturan Cepat untuk menerapkan jenis konfigurasi yang diperlukan untuk mengatur akses node just-in-time.

`AWSQuickSetupJITNADeploymentRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupJITNADeploymentRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 April 2025, 09:07 UTC
- Waktu teredit: 07 September 2026, 12:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupJITNADeploymentRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-JITNA-*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-JITNA-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack",
            "UpdateStack",
            "CreateChangeSet",
            "ExecuteChangeSet"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation",
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*::document/AWSQuickSetupType-SetupJITNAResources",
        "arn:aws:ssm:*::document/AWSQuickSetupType-
PropagateJustInTimeNodeAccessPolicies",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        },
        "StringEquals" : {
          "aws:CalledViaLast" : [
            "cloudformation.amazonaws.com"
          ],
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-JITNA"
          ],
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-JITNA"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
```

```
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::*:policy/AWSQuickSetupManageJITNAResourcesExecutionPolicy"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com",
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-JITNA"
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*::document/AWSQuickSetupType-SetupJITNAResources",
            "arn:aws:ssm:*:*:association/*"
          ]
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSetupManagedInstanceProfileExecutionPolicy

Deskripsi: Kebijakan ini memberikan izin administratif yang memungkinkan Manajer Sistem membuat profil instans IAM default untuk kemampuan Penyiapan Cepat dan melampirkannya ke instans Amazon EC2 yang belum memiliki instance. profil terlampir.

`AWSQuickSetupManagedInstanceProfileExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupManagedInstanceProfileExecutionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 November 2024, 21:51 UTC
- Waktu teredit: 03 Juni 2026, 14:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupManagedInstanceProfileExecutionPolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfilesForRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DefaultInstanceRoleManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
    },
    {
      "Sid" : "DefaultInstanceProfileCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : "iam:AddRoleToInstanceProfile",
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
```

```
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToEC2AndSSMPermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "InstanceManagementPoliciesAttachAmazonSSMManagedInstanceCore",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore",
            "arn:aws:iam::aws:policy/AmazonSSMPatchAssociation",
            "arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess",
            "arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils",
```

```
            "arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy"
          ]
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "InstanceProfileAssociationEc2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMInstanceManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:UpdateManagedInstanceRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagRoles",
      "Effect" : "Allow",
      "Action" : "iam:TagRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigId-*"
        }
      }
    },
    {
      "Sid" : "DenyModifyQuickSetupAutomationRoles",
      "Effect" : "Deny",
      "Action" : [
        "iam:TagRole",
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
    },
```

```
    {
      "Sid" : "AutomationsStartWithTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:document/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/InvokedBy" : [
            "AWSQuickSetupType-ManageInstanceProfile"
          ],
          "aws:ResourceTag/InvokedBy" : [
            "AWSQuickSetupType-ManageInstanceProfile"
          ]
        }
      }
    },
    {
      "Sid" : "AutomationsGetPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:GetAutomationExecution",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/InvokedBy" : [
            "AWSQuickSetupType-ManageInstanceProfile"
          ]
        }
      }
    },
    {
      "Sid" : "GetQuickSetupAutomationAssumeRoles",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM",
            "AWSQuickSetupType-SSMHostMgmt",
            "AWSQuickSetupType-PatchPolicy",
            "AWSQuickSetupType-Distributor",
            "AWSQuickSetupType-CWASetup"
          ]
        }
      }
    },
    {
      "Sid" : "PassQuickSetupAutomationAssumeRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM",
            "AWSQuickSetupType-SSMHostMgmt",
            "AWSQuickSetupType-PatchPolicy",
            "AWSQuickSetupType-Distributor",
            "AWSQuickSetupType-CWASetup"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSetupManageJITNAResourcesExecutionPolicy

Deskripsi: Kebijakan ini memberikan izin untuk mengaktifkan akses node tepat waktu untuk Manajer Sistem.

`AWSQuickSetupManageJITNAResourcesExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupManageJITNAResourcesExecutionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 April 2025, 21:37 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupManageJITNAResourcesExecutionPolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "CreateJustInTimeAccessServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/justintimeaccess.ssm.amazonaws.com/
AWSServiceRoleForSystemsManagerJustInTimeAccess"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "justintimeaccess.ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateSystemsManagerNotificationServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/notifications.ssm.amazonaws.com/
AWSServiceRoleForSystemsManagerNotifications"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "notifications.ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/SSM-JustInTimeAccessTokenRole",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::*:policy/
AWSSystemsManagerJustInTimeAccessTokenPolicy"
        }
      }
    },
```

```
    {
      "Sid" : "IAMRoleManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole",
        "iam:TagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/SSM-JustInTimeAccessTokenRole"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-JITNA"
          ]
        }
      }
    },
    {
      "Sid" : "ServiceSettingsManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/just-in-time-access/identity-provider"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSetupPatchPolicyBaselineAccess

Deskripsi: Menyediakan izin baca-saja untuk mengakses garis dasar patch yang telah dikonfigurasi oleh administrator di saat ini Akun AWS atau organisasi menggunakan Pengaturan Cepat.

`AWSQuickSetupPatchPolicyBaselineAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupPatchPolicyBaselineAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juni 2024, 09:38 UTC
- Waktu teredit: 26 Juni 2024, 09:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QuickSetupPatchingBaselineOverridesS3SameAccountReadOnlyAccess",
```

```
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::aws-quicksetup-patchpolicy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : [
            "${aws:ResourceAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "QuickSetupPatchingBaselineOverridesS3OrganizationReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::aws-quicksetup-patchpolicy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalOrgID" : [
            "${aws:ResourceOrgID}"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSetupPatchPolicyDeploymentRolePolicy

Deskripsi: Menyediakan izin yang memungkinkan Pengaturan Cepat untuk membuat sumber daya yang terkait dengan konfigurasi kebijakan patch.

`AWSQuickSetupPatchPolicyDeploymentRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupPatchPolicyDeploymentRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juni 2024, 09:57 UTC
- Waktu teredit: 04 September 2026, 08:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyDeploymentRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CfnRead",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*"
      ]
    },
    {
      "Sid" : "RGroupsGet",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3BucketsList",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AccessLogsBucketManage",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:Put*",
```

```
        "s3:Get*",
        "s3:List*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:s3:::aws-quicksetup-patchpolicy-access-log-*"
      ]
    },
    {
      "Sid" : "LambdaManage",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:UpdateFunction*",
        "lambda:GetFunction",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:DeleteFunction",
        "lambda:InvokeFunction",
        "lambda:UntagResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      },
      "Resource" : [
        "arn:aws:lambda:*:*:function:baseline-overrides-*",
```

```
        "arn:aws:lambda:*:*:function:delete-name-tags-*"
      ]
    },
    {
      "Sid" : "LogGroupsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LogGroupsManage",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource",
        "logs:PutRetentionPolicy",
        "logs:DeleteLogGroup",
        "logs:ListTagsForResource",
        "logs:UntagResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/baseline-overrides-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/delete-name-tags-*"
      ]
    },
    {
      "Sid" : "QSDocsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument",
        "ssm:UpdateDocument",
        "ssm:DescribeDocument",
        "ssm:UpdateDocumentDefaultVersion",
        "ssm:DeleteDocument",
        "ssm:AddTagsToResource",
```

```
        "ssm:RemoveTagsFromResource",
        "ssm:ListTagsForResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/QuickSetup-*"
      ]
    },
    {
      "Sid" : "QSDocsGet",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/QuickSetup-*",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-RunPatchBaseline"
      ]
    },
    {
      "Sid" : "QSAssociationsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
```

```
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/QuickSetup-*",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-RunPatchBaseline",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "SSMSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConfigRoleManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole",
        "iam:GetRole",
        "iam:UpdateRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
```

```
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ]
    },
    {
      "Sid" : "ConfigRolePassToSSM",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConfigRolePassToLambda",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DocDescribe",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:DescribeDocument"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LegacyDocClean",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteDocument"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
    {
      "Sid" : "LegacyIAMClean",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/*QuickSetup-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
    {
      "Sid" : "ConfigRoleBoundedManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePolicy",
        "iam:PutRolePermissionsBoundary"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AWSQuickSetupPatchPolicyPermissionsBoundary"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ]
    },
    {
      "Sid" : "CfnTagOnMutate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack",
            "UpdateStack",
            "CreateChangeSet",
            "ExecuteChangeSet"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSetupPatchPolicyLambdaExecutionPolicy

Deskripsi: Memberikan izin untuk mengelola asosiasi State Manager untuk operasi pembersihan otomatis saat konfigurasi Quick Setup dihapus.

`AWSQuickSetupPatchPolicyLambdaExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupPatchPolicyLambdaExecutionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Juni 2026, 14:12 UTC
- Waktu teredit: 03 Juni 2026, 14:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyLambdaExecutionPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageSSMAssociations",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociationExecutions",
        "ssm:UpdateAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-*"
      ]
    },
    {
      "Sid" : "PassQuickSetupAutomationRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSetupPatchPolicyPermissionsBoundary

Deskripsi QuickSetup : membuat peran IAM yang memungkinkannya untuk mengonfigurasi fitur Manajer Patch Manager Sistem atas nama Anda, dan menggunakan kebijakan ini saat membuat peran tersebut untuk menentukan batas izin mereka.

`AWSQuickSetupPatchPolicyPermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupPatchPolicyPermissionsBoundary` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juni 2024, 09:46 UTC
- Waktu teredit: 05 Maret 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyPermissionsBoundary`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PatchingAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
      ]
    },
    {
      "Sid" : "PatchingAutomationRolePassPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:UpdateRole",
        "iam:GetRole"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PoliciesAttachPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore",
            "arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess"
          ]
        },
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "CreateSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ManagedInstanceRoleUpdatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateManagedInstanceRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "InstanceProfileCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
```

```
    },
    {
      "Sid" : "InstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "InstanceProfileDisassociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "SSMAssociationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociationExecutions",
        "ssm:UpdateAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
```

```
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "BaselineS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:Put*",
        "s3:Get*",
        "s3:List*",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:DeleteBucket"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      },
      "Resource" : "arn:aws:s3:::aws-quicksetup-patchpolicy-*"
    },
    {
      "Sid" : "PatchingFunctionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:baseline-overrides-*",
        "arn:aws:lambda:*:*:function:delete-name-tags-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "LoggingPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/baseline-overrides-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/delete-name-tags-*"
      ]
    },
    {
      "Sid" : "SSMTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        }
      }
    },
    {
      "Sid" : "EC2TaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        }
      }
    },
    {
      "Sid" : "RoleTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
```

```
        "iam:UntagRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigId-*"
        }
      }
    },
    {
      "Sid" : "PatchingReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetPatchBaseline",
        "ssm:GetInventory",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeAssociation",
        "ssm:GetAutomationExecution",
        "ssm:ListTagsForResource",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PatchingAutomationsStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-EnableExplorer*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RunPatchBaseline*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:automation-definition/QuickSetup-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWS-EnableExplorer*",
        "arn:aws:ssm:*:*:document/AWS-RunPatchBaseline*",
        "arn:aws:ssm:*:*:document/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:document/QuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ]
    },
```

```
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSetupPatchPolicyTagManagementExecutionPolicy

Deskripsi: Memberikan izin untuk melacak instans mana yang dikelola oleh konfigurasi kebijakan patch Penyiapan Cepat melalui penandaan otomatis dan pengumpulan inventaris.

`AWSQuickSetupPatchPolicyTagManagementExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupPatchPolicyTagManagementExecutionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Juni 2026, 14:12 UTC
- Waktu teredit: 03 Juni 2026, 14:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyTagManagementExecutionPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GetSSMInventory",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetInventory"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageSSMManagedInstanceTags",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        },
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        }
      }
    },
    {
      "Sid" : "ManageEC2InstanceTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        },
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSetupSchedulerPermissionsBoundary

Deskripsi: AWSQuickSetupSchedulerPermissionsBoundary Kebijakan menentukan daftar izin yang diizinkan dalam peran IAM yang dibuat oleh Pengaturan Cepat. Penyiapan Cepat menggunakan peran yang dibuat dengan kebijakan ini untuk mengaktifkan dan mengonfigurasi operasi terjadwal pada instans Amazon EC2 dan sumber daya lainnya.

`AWSQuickSetupSchedulerPermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupSchedulerPermissionsBoundary` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juni 2024, 09:53 UTC
- Waktu teredit: 26 Juni 2024, 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSchedulerPermissionsBoundary`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "ConfigurationAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-Scheduler-*"
      ]
    },
    {
      "Sid" : "ConfigurationAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-Scheduler-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SystemsManagerCalendarReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCalendarState"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-ChangeCalendar-*"
      ]
    },
    {
      "Sid" : "EC2ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeRegions",
```

```
        "ec2:DescribeTags",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2StartStopPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AutomationStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
StartStateManagerAssociations-*"
      ]
    },
    {
      "Sid" : "AssociationsStartOncePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAssociationsOnce"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSetupSSMDeploymentRolePolicy

Deskripsi: Kebijakan ini memberikan izin administratif yang memungkinkan Pengaturan Cepat untuk membuat sumber daya yang digunakan selama proses orientasi Manajer Sistem.

`AWSQuickSetupSSMDeploymentRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupSSMDeploymentRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 November 2024, 22:53 UTC
- Waktu teredit: 07 September 2026, 12:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMDeploymentRolePolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-SSM-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-SSM-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
```

```
            "CreateStack",
            "UpdateStack",
            "CreateChangeSet",
            "ExecuteChangeSet"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:TagResource"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ],
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ],
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "lambda:InvokeFunction",
        "lambda:DeleteFunction",
        "lambda:UpdateFunction*"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ],
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
```

```
        "ssm:DescribeAssociation",
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableAREX",
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableDHMC",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*::document/AWS-UpdateSSMAgent",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SSMSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-*",
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ],
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:UpdateRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-*",
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ],
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-LifecycleManagement-*"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/
AWSQuickSetupSSMLifecycleManagementExecutionPolicy"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageResources-*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupSSMManageResourcesExecutionPolicy"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-
AdministrationRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-
ExecutionRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-
OperationalAccountAdministrationRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-Automation-DiagnosisBucketPolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-
AdministrationRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup*"
      ],
      "Condition" : {
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*::document/AWSQuickSetupType-EnableAREX",
            "arn:aws:ssm:*::document/AWSQuickSetupType-EnableDHMC",
            "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
            "arn:aws:ssm:*::document/AWS-EnableExplorer",
            "arn:aws:ssm:*:*:association/*"
          ]
        },
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com",
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-LifecycleManagement*"
      ],
      "Condition" : {
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle-*"
          ]
        },
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com",
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "lambda:TagResource",
      "Resource" : [
        "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QuickSetup*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        },
        "StringLike" : {
          "aws:RequestTag/QuickSetupDocumentVersionName" : "*"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-*",
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QuickSetup*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        },
        "StringLike" : {
          "aws:RequestTag/QuickSetupDocumentVersionName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : "arn:aws:ssm:*::document/AWSQuickSetupType-SSM-ManageResources"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociationExecutions",
        "ssm:DescribeAssociationExecutionTargets",
        "ssm:GetAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageResources*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSetupSSMDeploymentS3BucketRolePolicy

Deskripsi: Kebijakan ini memberikan izin untuk mencantumkan semua bucket S3 dalam akun; dan untuk mengelola dan mengambil informasi tentang bucket tertentu di akun utama yang dikelola melalui AWS CloudFormation templat.

`AWSQuickSetupSSMDeploymentS3BucketRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupSSMDeploymentS3BucketRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 November 2024, 22:01 UTC
- Waktu teredit: 15 November 2024, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMDeploymentS3BucketRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketTagging",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketVersioning"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSetupSSMHostMgmtPermissionsBoundary

Deskripsi: Penyiapan Cepat membuat peran IAM yang memungkinkannya mengonfigurasi jenis Pengaturan Cepat Host Manager atas nama Anda, dan menggunakan kebijakan ini saat membuat peran tersebut untuk menentukan batas izin mereka.

`AWSQuickSetupSSMHostMgmtPermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupSSMHostMgmtPermissionsBoundary` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juni 2024, 09:48 UTC
- Waktu teredit: 26 Juni 2024, 09:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMHostMgmtPermissionsBoundary`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HostManagementAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
      ]
    },
    {
      "Sid" : "HostManagementAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRoleManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:UpdateRole",
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToEC2Permissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToSSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "InstanceManagementPoliciesAttachPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore",
            "arn:aws:iam::aws:policy/AmazonSSMPatchAssociation"
          ]
```

```
        },
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRoles"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceProfileDisassociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
```

```
      }
    },
    {
      "Sid" : "ConfigurationAutomationsStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-HostMgmt-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
CreateAndAttachIAMToInstance-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
UpdateExistingInstanceProfile-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
InstallAndManageCloudWatchDocument-*",
        "arn:aws:ssm:*:*:automation-definition/UpdateCloudWatchDocument-*",
        "arn:aws:ssm:*:*:automation-definition/AWSEC2-UpdateLaunchAgent-*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:automation-definition/AWS-GatherSoftwareInventory*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RunPatchBaselineAssociation*",
        "arn:aws:ssm:*:*:automation-definition/AWS-UpdateSSMAgent*"
      ]
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingHostManagementBySSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListTagsForResource",
        "ssm:GetAutomationExecution",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSetupSSMLifecycleManagementExecutionPolicy

Deskripsi: Kebijakan ini memberikan izin administratif yang memungkinkan Pengaturan Cepat menjalankan sumber daya AWS CloudFormation khusus pada peristiwa siklus hidup selama penerapan Pengaturan Cepat di Manajer Sistem.

`AWSQuickSetupSSMLifecycleManagementExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupSSMLifecycleManagementExecutionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 November 2024, 21:55 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMLifecycleManagementExecutionPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageResources*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-SSM-ManageResources*",
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-SSM-ManageResources*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/QuickSetupDocument" : "AWSQuickSetupType-SSM",
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSetupSSMManageResourcesExecutionPolicy

Deskripsi: Kebijakan ini memberikan izin yang memungkinkan Manajer Sistem membuat prasyarat seperti peran IAM yang diperlukan untuk orientasi Manajer Sistem.

`AWSQuickSetupSSMManageResourcesExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupSSMManageResourcesExecutionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 November 2024, 22:49 UTC
- Waktu teredit: 15 November 2024, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMManageResourcesExecutionPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableExplorer*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableDHMC*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageInstanceProfile*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableAREX*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM",
          "aws:RequestTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:UpdateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableExplorer*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableDHMC*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageInstanceProfile*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableAREX*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy"
          ]
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableExplorer*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupEnableDHMCExecutionPolicy"
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableDHMC*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupManagedInstanceProfileExecutionPolicy"
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageInstanceProfile*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupEnableAREXExecutionPolicy"
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableAREX*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:DeleteObject",
        "s3:ListBucketVersions",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSetupStartSSMAssociationsExecutionPolicy

Deskripsi: Kebijakan ini memberikan izin yang memungkinkan kepala sekolah menjalankan runbook AWSQuickSetupType-StartSSMAssociations Otomasi, yang memulai Asosiasi Manajer Negara.

`AWSQuickSetupStartSSMAssociationsExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupStartSSMAssociationsExecutionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Agustus 2025, 12:04 UTC
- Waktu teredit: 05 Maret 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupStartSSMAssociationsExecutionPolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-Scheduler-
ChangeCalendarState*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*:*:document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
            "arn:aws:ssm:*:*:automation-execution/*",
            "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-Scheduler-
ChangeCalendarState*"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSetupStartStopInstancesExecutionPolicy

Deskripsi: Kebijakan terkelola AWSQuickSetupStartStopInstancesExecutionPolicy memberikan izin untuk Pengaturan Cepat untuk memulai dan menghentikan instans Amazon EC2 sesuai jadwal. Kebijakan ini digunakan dengan jenis konfigurasi penjadwal Pengaturan Cepat.

`AWSQuickSetupStartStopInstancesExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSetupStartStopInstancesExecutionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Agustus 2025, 12:04 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupStartStopInstancesExecutionPolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeRegions",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCalendarState"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/AWSQuickSetup-ChangeCalendar*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAssociationsOnce",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-Scheduler-ApplyInstanceState",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-Scheduler-
ApplyInstanceState*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ApplyInstanceState",
            "arn:aws:ssm:*:*:association/*"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSightAssetBundleExportPolicy

Deskripsi: Menyediakan kumpulan izin yang diperlukan untuk melakukan Operasi Ek QuickSight spor Bundel Aset

`AWSQuickSightAssetBundleExportPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightAssetBundleExportPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Maret 2024, 21:31 UTC
- Waktu teredit: 27 Maret 2024, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightAssetBundleExportPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TagReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:ListTagsForResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:*/*"
    },
    {
      "Sid" : "DashboardReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dashboard/*"
    },
    {
      "Sid" : "AnalysisReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:analysis/*"
    },
    {
      "Sid" : "DataSetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:ListRefreshSchedules",
        "quicksight:DescribeDataSetPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*"
    },
    {
      "Sid" : "DataSourceReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSource",
```

```
        "quicksight:DescribeDataSourcePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:datasource/*"
    },
    {
      "Sid" : "ThemeReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:theme/*"
    },
    {
      "Sid" : "VPCConnectionReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeVPCConnection",
        "quicksight:ListVPCConnections"
      ],
      "Resource" : "arn:aws:quicksight:*:*:vpcConnection/*"
    },
    {
      "Sid" : "RefreshScheduleReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeRefreshSchedule"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*/refresh-schedule/*"
    },
    {
      "Sid" : "AssetBundleExportOperations",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAssetBundleExportJob",
        "quicksight:ListAssetBundleExportJobs",
        "quicksight:StartAssetBundleExportJob"
      ],
      "Resource" : "arn:aws:quicksight:*:*:asset-bundle-export-job/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSightAssetBundleImportPolicy

Deskripsi: Menyediakan kumpulan izin yang diperlukan untuk melakukan Operasi QuickSight Impor Bundel Aset

`AWSQuickSightAssetBundleImportPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightAssetBundleImportPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Maret 2024, 21:40 UTC
- Waktu teredit: 27 Maret 2024, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightAssetBundleImportPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TagWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:ListTagsForResource",
        "quicksight:TagResource",
        "quicksight:UntagResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:*/*"
    },
    {
      "Sid" : "DashboardWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDashboard",
        "quicksight:DeleteDashboard",
        "quicksight:DescribeDashboard",
        "quicksight:UpdateDashboard",
        "quicksight:UpdateDashboardPublishedVersion",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:UpdateDashboardPermissions",
        "quicksight:UpdateDashboardLinks"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dashboard/*"
    },
    {
      "Sid" : "AnalysisWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateAnalysis",
        "quicksight:DeleteAnalysis",
        "quicksight:DescribeAnalysis",
        "quicksight:UpdateAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:UpdateAnalysisPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:analysis/*"
    },
    {
      "Sid" : "DataSetWriteAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "quicksight:CreateDataSet",
        "quicksight:DeleteDataSet",
        "quicksight:DescribeDataSet",
        "quicksight:PassDataSet",
        "quicksight:UpdateDataSet",
        "quicksight:DeleteDataSetRefreshProperties",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:PutDataSetRefreshProperties",
        "quicksight:UpdateDataSetPermissions",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:ListRefreshSchedules"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*"
    },
    {
      "Sid" : "DataSourceWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSource",
        "quicksight:DescribeDataSource",
        "quicksight:DeleteDataSource",
        "quicksight:PassDataSource",
        "quicksight:UpdateDataSource",
        "quicksight:UpdateDataSourcePermissions",
        "quicksight:DescribeDataSourcePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:datasource/*"
    },
    {
      "Sid" : "ThemeWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateTheme",
        "quicksight:DeleteTheme",
        "quicksight:DescribeTheme",
        "quicksight:UpdateTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:UpdateThemePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:theme/*"
    },
    {
      "Sid" : "RefreshScheduleWriteAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "quicksight:CreateRefreshSchedule",
        "quicksight:DescribeRefreshSchedule",
        "quicksight:DeleteRefreshSchedule",
        "quicksight:UpdateRefreshSchedule"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*/refresh-schedule/*"
    },
    {
      "Sid" : "VPCConnectionWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:ListVPCConnections",
        "quicksight:CreateVPCConnection",
        "quicksight:DescribeVPCConnection",
        "quicksight:DeleteVPCConnection",
        "quicksight:UpdateVPCConnection"
      ],
      "Resource" : "arn:aws:quicksight:*:*:vpcConnection/*"
    },
    {
      "Sid" : "AssetBundleImportOperations",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAssetBundleImportJob",
        "quicksight:ListAssetBundleImportJobs",
        "quicksight:StartAssetBundleImportJob"
      ],
      "Resource" : "arn:aws:quicksight:*:*:asset-bundle-import-job/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuicksightAthenaAccess

Deskripsi: Akses Quicksight ke Athena API dan bucket S3 yang digunakan untuk hasil kueri Athena

`AWSQuicksightAthenaAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuicksightAthenaAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 09 Desember 2016, 02:31 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess`

Versi kebijakan

Versi kebijakan: v13 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGetQueryExecution",
        "athena:CancelQueryExecution",
        "athena:GetCatalogs",
        "athena:GetExecutionEngine",
        "athena:GetExecutionEngines",
        "athena:GetNamespace",
        "athena:GetNamespaces",
```

```
        "athena:GetQueryExecution",
        "athena:GetQueryExecutions",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetTable",
        "athena:GetTables",
        "athena:ListQueryExecutions",
        "athena:RunQuery",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "athena:ListWorkGroups",
        "athena:ListEngineVersions",
        "athena:GetWorkGroup",
        "athena:GetDataCatalog",
        "athena:GetDatabase",
        "athena:GetTableMetadata",
        "athena:ListDataCatalogs",
        "athena:ListDatabases",
        "athena:ListTableMetadata"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
```

```
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-athena-query-results-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSightDescribeRDS

Deskripsi: Izinkan QuickSight untuk menjelaskan sumber daya RDS

`AWSQuickSightDescribeRDS`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightDescribeRDS` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 10 November 2015, 23:24 UTC
- Waktu teredit: 10 November 2015, 23:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:Describe*"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSightDescribeRedshift

Deskripsi: Izinkan QuickSight untuk menjelaskan sumber daya Redshift

`AWSQuickSightDescribeRedshift`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightDescribeRedshift` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 10 November 2015, 23:25 UTC
- Waktu teredit: 10 November 2015, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "redshift:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSightElasticsearchPolicy

Deskripsi: Menyediakan akses ke sumber daya Amazon Elasticsearch dari Amazon QuickSight

`AWSQuickSightElasticsearchPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightElasticsearchPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 09 September 2020, 17:27 UTC

- Waktu teredit: 07 September 2021, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/",
        "arn:aws:es:*:*:domain/*/_cluster/settings",
        "arn:aws:es:*:*:domain/*/_cat/indices"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "es:ListDomainNames",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:DescribeElasticsearchDomain",
        "es:DescribeDomain"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpPost",
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/_opendistro/_sql",
        "arn:aws:es:*:*:domain/*/_plugin/_sql"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSightIoTAnalyticsAccess

Deskripsi: Memberikan akses QuickSight baca-saja ke kumpulan data IoT Analytics

`AWSQuickSightIoTAnalyticsAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightIoTAnalyticsAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2017, 17:00 UTC
- Waktu teredit: 29 November 2017, 17:00 UTC

- ARN: `arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iotanalytics:ListDatasets",
        "iotanalytics:DescribeDataset",
        "iotanalytics:GetDatasetContent"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSightListIAM

Deskripsi: Izinkan QuickSight untuk mencantumkan entitas IAM

`AWSQuickSightListIAM`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightListIAM` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 10 November 2015, 23:25 UTC
- Waktu teredit: 10 November 2015, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuicksightOpenSearchPolicy

Deskripsi: Menyediakan akses ke OpenSearch sumber daya Amazon dari Amazon QuickSight

`AWSQuicksightOpenSearchPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuicksightOpenSearchPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 September 2021, 23:26 UTC
- Waktu teredit: 07 September 2021, 23:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/",
        "arn:aws:es:*:*:domain/*/_cluster/settings",
        "arn:aws:es:*:*:domain/*/_cat/indices"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "es:ListDomainNames",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:DescribeDomain"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpPost",
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/_opendistro/_sql",
        "arn:aws:es:*:*:domain/*/_plugin/_sql"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSightSageMakerPolicy

Deskripsi: Menyediakan akses ke SageMaker sumber daya Amazon dari Amazon QuickSight

`AWSQuickSightSageMakerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightSageMakerPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 17 Januari 2020, 17:18 UTC
- Waktu teredit: 30 Oktober 2023, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerTransformJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
        "sagemaker:CreateTransformJob"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:transform-job/quicksight-auto-generated-*"
```

```
    },
    {
      "Sid" : "SageMakerModelReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListModels",
        "sagemaker:DescribeModel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ObjectReadAccess",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::quicksight-ml.*",
        "arn:aws:s3:::sagemaker*"
      ]
    },
    {
      "Sid" : "S3ObjectUpdateAccess",
      "Effect" : "Allow",
      "Action" : "s3:PutObject",
      "Resource" : "arn:aws:s3:::sagemaker*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3BucketReadAccess",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::sagemaker*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSightSecretsManagerWriteAccess

Deskripsi: Kebijakan yang digunakan QuickSight untuk membuat rahasia di Manajer AWS Rahasia dan untuk melampirkan kebijakan sumber daya pada QuickSight rahasia yang ada.

`AWSQuickSightSecretsManagerWriteAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightSecretsManagerWriteAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 Mei 2025, 01:22 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSecretsManagerWriteAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "quicksight",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "secretsmanager:Name" : "quicksight!*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSightSecretsManagerWritePolicy

Deskripsi: Kebijakan yang digunakan QuickSight untuk membuat rahasia di Manajer AWS Rahasia dan untuk melampirkan kebijakan sumber daya pada QuickSight rahasia yang ada.

`AWSQuickSightSecretsManagerWritePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightSecretsManagerWritePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Mei 2025, 19:22 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightSecretsManagerWritePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "quicksight",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "secretsmanager:Name" : "quicksight!*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSQuickSightTimestreamPolicy

Deskripsi: AWS QuickSight akses ke API AWS Timestream. Pelanggan dapat melampirkan kebijakan ini ke AWS QuickSight role untuk memungkinkan pengambilan data dan metadata.

`AWSQuickSightTimestreamPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightTimestreamPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 30 September 2020, 21:47 UTC
- Waktu teredit: 30 September 2020, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:Select",
        "timestream:CancelQuery",
        "timestream:ListTables",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase",
        "timestream:SelectValues",
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSReachabilityAnalyzerServiceRolePolicy

Deskripsi: Mengizinkan VPC Reachability Analyzer mengakses AWS sumber daya dan berintegrasi dengan AWS Organisasi atas nama Anda.

`AWSReachabilityAnalyzerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 23 November 2022, 17:12 UTC
- Waktu teredit: 14 Agustus 2026, 17:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReachabilityAnalyzerPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:GetTransitGatewayPolicyTableEntries",
        "ec2:GetTransitGatewayPolicyTableAssociations",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeAddresses",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
```

```
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallMetadata",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "tag:GetResources",
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApigatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSRefactoringToolkitFullAccess

Deskripsi: Kebijakan ini memberikan izin untuk menggunakan AWS layanan dengan ekstensi AWS Toolkit untuk .NET Refactoring untuk Microsoft Visual Studio. Ini dimaksudkan untuk dilampirkan ke AWS profil lokal. Kebijakan ini memungkinkan mengunggah artefak aplikasi dan mengunduh artefak yang dihasilkan dari Amazon S3. Ini memungkinkan membangun aplikasi ke dalam gambar wadah menggunakan AWS CodeBuild dan menyimpan dan mengambil gambar dari Amazon Elastic Container Registry (Amazon ECR). Dan ini memungkinkan penyebaran aplikasi ke layanan kontainer AWS seperti Amazon Elastic Container Service (Amazon ECS), pembuatan opsional sumber daya VPC, koneksi opsional ke infrastruktur yang ada seperti Layanan AWS Direktori, dan layanan terkait lainnya.

`AWSRefactoringToolkitFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSRefactoringToolkitFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Oktober 2022, 16:41 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a2c:GetContainerizationJobDetails",
        "a2c:GetDeploymentJobDetails",
        "a2c:StartContainerizationJob",
        "a2c:StartDeploymentJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:UpdateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:*:cloudformation:*:*:stack/a2c-app-*",
        "arn:*:cloudformation:*:*:stack/a2c-build-*",
        "arn:*:cloudformation:*:*:stack/application-transformation-app-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:UpdateProject"
      ],
```

```
      "Resource" : "arn:aws:codebuild:*:*:project/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:StartBuild"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
```

```
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-transformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "AuthorizeSecurityGroupIngress",
            "CreateInternetGateway",
            "CreateKeyPair",
            "CreateRoute",
            "CreateRouteTable",
            "CreateSubnet",
            "CreateVpc"
          ]
```

```
        },
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-transformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteTags",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteTags",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
```

```
        "ec2:CreateRouteTable"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetLifecyclePolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecr:TagResource",
        "ecr:UntagResource"
```

```
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetLifecyclePolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:CreateService",
        "ecs:RegisterTaskDefinition",
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
```

```
        "ecs:CreateService",
        "ecs:RegisterTaskDefinition",
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTaskDefinition"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:ExecuteCommand"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ecs:container-name" : "a2c-sidecar"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:ExecuteCommand"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ecs:container-name" : "application-transformation-sidecar"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "a2c-generated"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "application-transformation"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:GetParameters",
        "ssm:PutParameter",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/a2c-generated-check-ecs-slr-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeSessions",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
```

```
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/refactoringtoolkit*",
        "arn:aws:s3:::*/a2c-generated*",
        "arn:aws:s3:::*/application-transformation*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "application-transformation",
            "refactoringtoolkit"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "clouddirectory:ListDirectories",
        "codebuild:BatchGetProjects",
        "codebuild:BatchGetBuilds",
        "ds:DescribeDirectories",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
```

```
        "ec2:DescribeImages",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ecr:DescribeImages",
        "ecr:DescribeRepositories",
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ecs:DescribeTasks",
        "ecs:ListTagsForResource",
        "ecs:ListTasks",
        "iam:ListRoles",
        "s3:GetBucketLocation",
        "s3:GetBucketVersioning",
        "s3:ListAllMyBuckets",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws.portingassistant.dotnet.datastore",
        "arn:aws:s3:::aws.portingassistant.dotnet.datastore/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-transformation:StartPortingCompatibilityAssessment",
```

```
        "application-transformation:GetPortingCompatibilityAssessment",
        "application-transformation:StartPortingRecommendationAssessment",
        "application-transformation:GetPortingRecommendationAssessment",
        "application-transformation:PutLogData",
        "application-transformation:PutMetricData",
        "application-transformation:StartContainerization",
        "application-transformation:GetContainerization",
        "application-transformation:StartDeployment",
        "application-transformation:GetDeployment"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*::*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : "alias/application-transformation*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "ecr:ResourceTag/application-transformation" : "false"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*::*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : "alias/application-transformation*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSRefactoringToolkitSidecarPolicy

Deskripsi: Kebijakan ini dimaksudkan untuk digunakan oleh Amazon ECS Tasks yang dibuat untuk menguji aplikasi dalam AWS menggunakan ekstensi AWS Toolkit untuk .NET Refactoring untuk Microsoft Visual Studio. Kebijakan ini memberikan akses untuk mengunduh artefak aplikasi dari Amazon S3, mengkomunikasikan status Tugas menggunakan Manajer AWS Sistem, dan layanan lain yang diperlukan.

`AWSRefactoringToolkitSidecarPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSRefactoringToolkitSidecarPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Oktober 2022, 16:41 UTC
- Waktu teredit: 29 Oktober 2022, 22.15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SsmMessagesAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenControlChannel",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssmmessages:CreateDataChannel"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "S3GetObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/refactoringtoolkit*"
    },
    {
      "Sid" : "S3ListBucketAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : "refactoringtoolkit*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSrePostPrivateCloudWatchAccess

Deskripsi: Menyediakan akses pribadi re:Post untuk mempublikasikan data metrik CloudWatch

`AWSrePostPrivateCloudWatchAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 15 November 2023, 16:37 UTC
- Waktu teredit: 15 November 2023, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSrePostPrivateCloudWatchAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchPublishMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/rePostPrivate",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSRepostSpaceSupportOperationsPolicy

Deskripsi: Kebijakan ini memungkinkan layanan Re:Post Space untuk membuat, mengelola, dan menyelesaikan kasus Dukungan yang dibuat melalui aplikasi Space.

`AWSRepostSpaceSupportOperationsPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSRepostSpaceSupportOperationsPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 November 2023, 21:52 UTC
- Waktu teredit: 26 November 2023, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "RepostSpaceSupportOperations",
      "Effect" : "Allow",
      "Action" : [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSResilienceHubAsssessmentExecutionPolicy

Deskripsi: Kebijakan untuk AWS peran layanan Resilience Hub yang memungkinkan akses ke AWS layanan lain untuk melaksanakan penilaian.

`AWSResilienceHubAsssessmentExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSResilienceHubAsssessmentExecutionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2023, 12:32 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC

- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubAsssessmentExecutionPolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubFullResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:DescribeBackupVault",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ValidateTemplate",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "datasync:DescribeTask",
        "datasync:ListLocations",
        "datasync:ListTasks",
        "devops-guru:ListMonitoredResources",
        "dlm:GetLifecyclePolicies",
        "dlm:GetLifecyclePolicy",
        "docdb-elastic:GetCluster",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:ListTagsForResource",
```

```
        "drs:DescribeJobs",
        "drs:DescribeSourceServers",
        "drs:GetReplicationConfiguration",
        "ds:DescribeDirectories",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DescribeFleets",
        "ec2:DescribeHosts",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ecr:DescribeRegistry",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodegroup",
        "eks:ListFargateProfiles",
        "eks:ListNodegroups",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeServerlessCaches",
        "elasticache:DescribeServerlessCacheSnapshots",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
```

```
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "fis:GetExperiment",
        "fis:GetExperimentTemplate",
        "fis:ListExperimentTemplates",
        "fis:ListExperiments",
        "fis:ListExperimentResolvedTargets",
        "fsx:DescribeFileSystems",
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:ListAliases",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListVersionsByFunction",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSnapshots",
        "rds:DescribeGlobalClusters",
        "rds:ListTagsForResource",
        "resource-groups:GetGroup",
        "resource-groups:ListGroupResources",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverEndpointIpAddresses",
        "s3:ListBucket",
        "servicecatalog:GetApplication",
        "servicecatalog:ListAssociatedResources",
```

```
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "ssm:DescribeAutomationExecutions",
        "states:DescribeStateMachine",
        "states:ListStateMachineVersions",
        "states:ListStateMachineAliases",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSResilienceHubApiGatewayStatement",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/usageplans"
      ]
    },
    {
      "Sid" : "AWSResilienceHubS3ArtifactStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::aws-resilience-hub-artifacts-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubS3AccessStatement",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetMultiRegionAccessPointRoutes",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubCloudWatchStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "ResilienceHub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubSSMStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ResilienceHub/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSResilienceHubResilienceTestingPolicy

Deskripsi: Kebijakan untuk peran layanan AWS Resilience Hub yang memungkinkan akses ke AWS Layanan Injeksi Kesalahan untuk memulai pengujian ketahanan.

`AWSResilienceHubResilienceTestingPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSResilienceHubResilienceTestingPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 31 Juli 2026, 22:27 UTC
- Waktu teredit: 31 Juli 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubResilienceTestingPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubFISActionStatement",
      "Effect" : "Allow",
      "Action" : "fis:CreateExperimentTemplate",
      "Resource" : "arn:aws:fis:*:*:action/*"
    },
    {
      "Sid" : "AWSResilienceHubFISCreateExperimentTemplateStatement",
      "Effect" : "Allow",
      "Action" : "fis:CreateExperimentTemplate",
      "Resource" : "arn:aws:fis:*:*:experiment-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedBy" : "resiliencehub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubFISStartExperimentFromTemplateStatement",
      "Effect" : "Allow",
      "Action" : "fis:StartExperiment",
      "Resource" : "arn:aws:fis:*:*:experiment-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/managedBy" : "resiliencehub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubFISStartExperimentStatement",
      "Effect" : "Allow",
      "Action" : "fis:StartExperiment",
      "Resource" : "arn:aws:fis:*:*:experiment/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedBy" : "resiliencehub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubFISExperimentStatement",
      "Effect" : "Allow",
```

```
      "Action" : [
        "fis:GetExperiment",
        "fis:StopExperiment",
        "fis:ListExperimentResolvedTargets"
      ],
      "Resource" : "arn:aws:fis:*:*:experiment/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/managedBy" : "resiliencehub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubFISExperimentTemplateStatement",
      "Effect" : "Allow",
      "Action" : [
        "fis:CreateTargetAccountConfiguration",
        "fis:DeleteExperimentTemplate"
      ],
      "Resource" : "arn:aws:fis:*:*:experiment-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/managedBy" : "resiliencehub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubFISPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "fis.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubFISTagResourceStatement",
      "Effect" : "Allow",
      "Action" : "fis:TagResource",
      "Resource" : [
        "arn:aws:fis:*:*:experiment-template/*",
        "arn:aws:fis:*:*:experiment/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedBy" : "resiliencehub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubRegionSwitchStatement",
      "Effect" : "Allow",
      "Action" : [
        "arc-region-switch:ListPlanExecutions",
        "arc-region-switch:GetPlanExecution"
      ],
      "Resource" : "arn:aws:arc-region-switch::*:plan/*:*"
    },
    {
      "Sid" : "AWSResilienceHubFISCreateSLRStatement",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "fis.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubCloudWatchAlarmStatement",
      "Effect" : "Allow",
      "Action" : "cloudwatch:DescribeAlarmHistory",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSResilienceHubServiceRolePolicy

Deskripsi: Men AWS gizinkan Resilience Hub mengakses sumber daya di akun Anda untuk penemuan, penilaian, dan pengelolaan ketahanan.

`AWSResilienceHubServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 28 Mei 2026, 17:42 UTC
- Waktu teredit: 06 Juli 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResilienceHubServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubOrganizationsReadStatement",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
```

```
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots",
        "organizations:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSResilienceHubV2AssessmentExecutionPolicy

Deskripsi: Men AWS gizinkan Resilience Hub mengakses sumber daya di akun Anda untuk penemuan, penilaian, dan pengelolaan ketahanan. Kebijakan ini memberikan izin baca-saja dengan karakter pengganti yang mungkin menyertakan informasi sensitif dalam output.

`AWSResilienceHubV2AssessmentExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSResilienceHubV2AssessmentExecutionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Juni 2026, 22:57 UTC
- Waktu teredit: 17 Juni 2026, 22:57 UTC

- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubV2AssessmentExecutionPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubV2ReadResourceConfigStatement",
      "Effect" : "Allow",
      "Action" : [
        "acm:Describe*",
        "acm:List*",
        "application-autoscaling:Describe*",
        "application-autoscaling:GetPredictiveScalingForecast",
        "application-autoscaling:ListTagsForResource",
        "arc-region-switch:Get*",
        "arc-region-switch:List*",
        "arc-zonal-shift:Get*",
        "arc-zonal-shift:List*",
        "autoscaling:Describe*",
        "autoscaling:GetPredictiveScalingForecast",
        "backup:Describe*",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:List*",
        "cloudformation:Describe*",
        "cloudformation:GetResource",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
```

```
        "cloudformation:List*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "config:Describe*",
        "config:GetStoredQuery",
        "config:List*",
        "datasync:Describe*",
        "datasync:List*",
        "dlm:Get*",
        "docdb-elastic:Get*",
        "docdb-elastic:List*",
        "drs:Describe*",
        "drs:Get*",
        "drs:List*",
        "ds:Describe*",
        "dsql:Get*",
        "dsql:List*",
        "dynamodb:Describe*",
        "dynamodb:GetResourcePolicy",
        "dynamodb:List*",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeClientVpnConnections",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
```

```
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ecr:Describe*",
        "ecs:Describe*",
        "ecs:List*",
        "eks:Describe*",
        "eks:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticfilesystem:Describe*",
        "elasticfilesystem:ListTagsForResource",
        "elasticloadbalancing:Describe*",
        "events:Describe*",
        "events:List*",
        "firehose:Describe*",
        "firehose:List*",
        "fis:Get*",
        "fis:List*",
```

```
        "fsx:Describe*",
        "fsx:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "iam:GetInstanceProfile",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListRoleTags",
        "kafka:Describe*",
        "kafka:GetClusterPolicy",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kinesis:Describe*",
        "kinesis:List*",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:List*",
        "memorydb:Describe*",
        "memorydb:List*",
        "network-firewall:Describe*",
        "network-firewall:List*",
        "qldb:Describe*",
        "qldb:List*",
        "ram:Get*",
        "ram:List*",
        "rds:Describe*",
```

```
        "rds:List*",
        "redshift:Describe*",
        "redshift:List*",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "route53-recovery-cluster:Get*",
        "route53-recovery-cluster:List*",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:Get*",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:Get*",
        "route53-recovery-readiness:List*",
        "route53:Get*",
        "route53:List*",
        "route53domains:Check*",
        "route53domains:List*",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3:ListBucket",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecrets",
        "servicecatalog:GetApplication",
        "servicecatalog:ListAssociatedResources",
        "shield:Describe*",
        "shield:Get*",
        "shield:List*",
        "sns:GetDataProtectionPolicy",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:List*",
        "ssm:Describe*",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetMaintenanceWindow",
        "ssm:GetParameters",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:List*",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
```

```
        "ssm-incidents:List*",
        "states:Describe*",
        "states:List*",
        "tag:GetResources",
        "vpc-lattice:Get*",
        "vpc-lattice:List*",
        "wafv2:Get*",
        "wafv2:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSResilienceHubApiGatewayStatement",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/domainnames/*"
      ]
    },
    {
      "Sid" : "AWSResilienceHubS3AccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetMultiRegionAccessPointRoutes",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSResourceAccessManagerFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Resource Access Manager

`AWSResourceAccessManagerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSResourceAccessManagerFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Juni 2019, 17:28 UTC
- Waktu teredit: 04 Juni 2019, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ram:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSResourceAccessManagerReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke AWS Resource Access Manager.

`AWSResourceAccessManagerReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSResourceAccessManagerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Desember 2019, 20:58 UTC
- Waktu teredit: 09 Desember 2019, 20:58 UTC

- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ram:Get*",
        "ram:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSResourceAccessManagerResourceShareParticipantAccess

Deskripsi: Menyediakan akses ke API AWS Resource Access Manager yang dibutuhkan oleh peserta berbagi sumber daya.

`AWSResourceAccessManagerResourceShareParticipantAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSResourceAccessManagerResourceShareParticipantAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Desember 2019, 20:41 UTC
- Waktu teredit: 09 Desember 2019, 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerResourceShareParticipantAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourcePolicies",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShares",
        "ram:ListPendingInvitationResources",
        "ram:ListPrincipals",
        "ram:ListResources",
        "ram:RejectResourceShareInvitation"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSResourceAccessManagerServiceRolePolicy

Deskripsi: Kebijakan yang berisi akses Read-only AWS Resource Access Manager ke struktur Organisasi pelanggan. Hal ini juga berisi izin IAM untuk menghapus peran.

`AWSResourceAccessManagerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 14 November 2018, 19:28 UTC
- Waktu teredit: 14 November 2018, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDeletionOfServiceLinkedRoleForResourceAccessManager",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ram.amazonaws.com/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSResourceExplorerFullAccess

Deskripsi: Kebijakan ini memberikan izin administratif untuk mengakses sumber daya Resource Explorer dan memberikan izin baca-saja ke AWS layanan lain untuk mendukung akses ini.

`AWSResourceExplorerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSResourceExplorerFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 November 2022, 20:01 UTC
- Waktu teredit: 14 November 2023, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerConsoleFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:*",
```

```
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceExplorerSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSResourceExplorerOrganizationsAccess

Deskripsi: Kebijakan ini memberikan izin administratif ke Resource Explorer dan memberikan izin baca-saja ke AWS layanan lain untuk mendukung akses ini. Administrator AWS Organisasi memerlukan izin ini untuk mengatur dan mengelola pencarian multi-akun di konsol.

`AWSResourceExplorerOrganizationsAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSResourceExplorerOrganizationsAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 November 2023, 17:01 UTC
- Waktu teredit: 14 November 2023, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:*",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceExplorerGetSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer"
    },
    {
      "Sid" : "ResourceExplorerCreateSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationsAdministratorAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSResourceExplorerReadOnlyAccess

Deskripsi: Kebijakan ini memberikan izin baca-saja untuk mencari dan melihat sumber daya Resource Explorer dan memberikan izin baca-saja ke AWS layanan lain untuk mendukung akses ini.

`AWSResourceExplorerReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSResourceExplorerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 November 2022, 19:56 UTC
- Waktu teredit: 14 November 2023, 16:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:Get*",
        "resource-explorer-2:List*",
        "resource-explorer-2:Search",
        "resource-explorer-2:BatchGetView",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSResourceExplorerServiceRolePolicy

Deskripsi: Mengizinkan Resource Explorer untuk melihat sumber daya dan CloudTrail acara atas nama Anda untuk mengindeks sumber daya Anda untuk pencarian.

`AWSResourceExplorerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 25 Oktober 2022, 20:35 UTC
- Waktu teredit: 01 Oktober 2026, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v56 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerAndOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:CreateView",
        "resource-explorer-2:AssociateDefaultView",
        "resource-explorer-2:DeleteIndex",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
```

```
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudTrailEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:GetServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/resource-
explorer-2/*"
    },
    {
      "Sid" : "ApiGatewayAccess",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*"
      ]
    },
    {
      "Sid" : "ResourceInventoryAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ValidatePolicy",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:ListEnvironments",
        "amplify:GetDomainAssociation",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListTagsForResource",
        "amplifyuibuilder:GetComponent",
        "amplifyuibuilder:ListComponents",
        "amplifyuibuilder:ListForms",
        "aoss:BatchGetCollection",
        "aoss:BatchGetCollectionGroup",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollectionGroups",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListTagsForResource",
        "aoss:ListVpcEndpoints",
        "app-integrations:GetApplication",
        "app-integrations:GetDataIntegration",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListApplications",
        "app-integrations:ListDataIntegrations",
        "app-integrations:ListEventIntegrations",
```

```
        "app-integrations:ListTagsForResource",
        "appconfig:GetExtension",
        "appconfig:ListApplications",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListExtensions",
        "appflow:DescribeConnector",
        "appflow:DescribeFlow",
        "appflow:ListConnectors",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScheduledActions",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServices",
        "application-signals:ListTagsForResource",
        "applicationinsights:DescribeApplication",
        "applicationinsights:DescribeComponent",
        "applicationinsights:DescribeLogPattern",
        "applicationinsights:ListApplications",
        "applicationinsights:ListComponents",
        "applicationinsights:ListLogPatternSets",
        "applicationinsights:ListLogPatterns",
        "applicationinsights:ListTagsForResource",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListServices",
        "apprunner:ListVpcConnectors",
```

```
        "apprunner:ListVpcIngressConnections",
        "appstream:DescribeAppBlockBuilders",
        "appstream:DescribeAppBlocks",
        "appstream:DescribeApplications",
        "appstream:DescribeFleets",
        "appstream:DescribeImageBuilders",
        "appstream:DescribeStacks",
        "appstream:ListAssociatedFleets",
        "appstream:ListAssociatedStacks",
        "appstream:ListTagsForResource",
        "appsync:GetApi",
        "appsync:GetApiAssociation",
        "appsync:GetApiCache",
        "appsync:GetChannelNamespace",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
        "appsync:GetGraphqlApi",
        "appsync:GetResolver",
        "appsync:GetSourceApiAssociation",
        "appsync:ListApis",
        "appsync:ListChannelNamespaces",
        "appsync:ListDataSources",
        "appsync:ListDomainNames",
        "appsync:ListGraphqlApis",
        "appsync:ListResolvers",
        "appsync:ListSourceApiAssociations",
        "appsync:ListTagsForResource",
        "appsync:ListTypes",
        "apptest:GetTestCase",
        "apptest:ListTagsForResource",
        "apptest:ListTestCases",
        "aps:DescribeAnomalyDetector",
        "aps:DescribeQueryLoggingConfiguration",
        "aps:DescribeResourcePolicy",
        "aps:DescribeRuleGroupsNamespace",
        "aps:DescribeScraper",
        "aps:DescribeScraperLoggingConfiguration",
        "aps:DescribeWorkspaceConfiguration",
        "aps:ListAnomalyDetectors",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListScrapers",
        "aps:ListTagsForResource",
        "aps:ListWorkspaces",
        "arc-region-switch:GetPlan",
```

```
        "arc-region-switch:ListPlans",
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListTagsForResource",
        "arc-zonal-shift:GetAutoshiftObserverNotificationStatus",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:ListManagedResources",
        "athena:GetCapacityAssignmentConfiguration",
        "athena:GetCapacityReservation",
        "athena:ListCapacityReservations",
        "athena:ListDataCatalogs",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:GetAssessmentFramework",
        "auditmanager:GetControl",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessments",
        "auditmanager:ListControls",
        "auditmanager:ListTagsForResource",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "b2bi:GetCapability",
        "b2bi:GetPartnership",
        "b2bi:GetProfile",
        "b2bi:ListCapabilities",
        "b2bi:ListPartnerships",
        "b2bi:ListProfiles",
        "b2bi:ListTagsForResource",
        "backup-gateway:GetHypervisor",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupVaults",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListReportPlans",
        "backup:ListRestoreTestingPlans",
        "backup:ListRestoreTestingSelections",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeConsumableResource",
        "batch:DescribeJobDefinitions",
        "batch:DescribeJobQueues",
```

```
        "batch:DescribeQuotaShare",
        "batch:DescribeServiceEnvironments",
        "batch:ListConsumableResources",
        "batch:ListQuotaShares",
        "batch:ListSchedulingPolicies",
        "bcm-dashboards:GetDashboard",
        "bcm-dashboards:ListDashboards",
        "bcm-dashboards:ListTagsForResource",
        "bcm-data-exports:GetExport",
        "bcm-data-exports:ListExports",
        "bcm-data-exports:ListTagsForResource",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetApiKeyCredentialProvider",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetCodeInterpreter",
        "bedrock-agentcore:GetConfigurationBundle",
        "bedrock-agentcore:GetEvaluator",
        "bedrock-agentcore:GetGateway",
        "bedrock-agentcore:GetGatewayTarget",
        "bedrock-agentcore:GetMemory",
        "bedrock-agentcore:GetOauth2CredentialProvider",
        "bedrock-agentcore:GetOnlineEvaluationConfig",
        "bedrock-agentcore:GetPaymentConnector",
        "bedrock-agentcore:GetPaymentManager",
        "bedrock-agentcore:GetPolicy",
        "bedrock-agentcore:GetPolicyEngine",
        "bedrock-agentcore:GetPolicyEngineSummary",
        "bedrock-agentcore:GetPolicyGeneration",
        "bedrock-agentcore:GetPolicySummary",
        "bedrock-agentcore:GetResourcePolicy",
        "bedrock-agentcore:GetTokenVault",
        "bedrock-agentcore:GetWorkloadIdentity",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListApiKeyCredentialProviders",
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListConfigurationBundles",
        "bedrock-agentcore:ListEvaluators",
        "bedrock-agentcore:ListGatewayTargets",
        "bedrock-agentcore:ListGateways",
        "bedrock-agentcore:ListMemories",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "bedrock-agentcore:ListOnlineEvaluationConfigs",
```

```
        "bedrock-agentcore:ListPaymentConnectors",
        "bedrock-agentcore:ListPaymentManagers",
        "bedrock-agentcore:ListPolicies",
        "bedrock-agentcore:ListPolicyEngineSummaries",
        "bedrock-agentcore:ListPolicyEngines",
        "bedrock-agentcore:ListPolicyGenerations",
        "bedrock-agentcore:ListPolicySummaries",
        "bedrock-agentcore:ListWorkloadIdentities",
        "bedrock:GetAgentAlias",
        "bedrock:GetAutomatedReasoningPolicy",
        "bedrock:GetBlueprint",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataSource",
        "bedrock:GetEvaluationJob",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetFoundationModel",
        "bedrock:GetInferenceProfile",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgents",
        "bedrock:ListAutomatedReasoningPolicies",
        "bedrock:ListBlueprints",
        "bedrock:ListCustomModels",
        "bedrock:ListDataAutomationProjects",
        "bedrock:ListDataSources",
        "bedrock:ListEnforcedGuardrailsConfiguration",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlowVersions",
        "bedrock:ListFlows",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListPromptRouters",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "billing:GetBillingView",
        "billing:ListBillingViews",
        "billing:ListSourceViewsForBillingView",
        "billing:ListTagsForResource",
        "budgets:DescribeBudgetActionsForAccount",
```

```
        "budgets:ViewBudget",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:GetMicrosoftTeamsChannelConfiguration",
        "chatbot:ListMicrosoftTeamsChannelConfigurations",
        "chime:DescribeAppInstance",
        "chime:ListAppInstanceBots",
        "chime:ListAppInstanceUsers",
        "chime:ListAppInstances",
        "chime:ListMediaInsightsPipelineConfigurations",
        "chime:ListMediaPipelineKinesisVideoStreamPools",
        "chime:ListMediaPipelines",
        "chime:ListSipMediaApplications",
        "chime:ListTagsForResource",
        "chime:ListVoiceConnectors",
        "cleanrooms-ml:GetConfiguredModelAlgorithm",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetConfiguredTableAssociationAnalysisRule",
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListTagsForResource",
        "cloud9:ListEnvironments",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:DescribePublisher",
```

```
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeType",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:ListResources",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSets",
        "cloudformation:ListStacks",
        "cloudformation:ListTypes",
        "cloudfront:DescribeFunction",
        "cloudfront:DescribeKeyValueStore",
        "cloudfront:GetAnycastIpList",
        "cloudfront:GetCachePolicy",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetConnectionGroup",
        "cloudfront:GetContinuousDeploymentPolicy",
        "cloudfront:GetDistributionTenant",
        "cloudfront:GetKeyGroup",
        "cloudfront:GetMonitoringSubscription",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetOriginRequestPolicy",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetVpcOrigin",
        "cloudfront:ListAnycastIpLists",
        "cloudfront:ListCachePolicies",
        "cloudfront:ListCloudFrontOriginAccessIdentities",
        "cloudfront:ListConnectionGroups",
        "cloudfront:ListContinuousDeploymentPolicies",
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListDistributions",
        "cloudfront:ListFieldLevelEncryptionConfigs",
        "cloudfront:ListFieldLevelEncryptionProfiles",
        "cloudfront:ListFunctions",
        "cloudfront:ListKeyGroups",
        "cloudfront:ListKeyValueStores",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListOriginRequestPolicies",
        "cloudfront:ListPublicKeys",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
```

```
        "cloudfront:ListVpcOrigins",
        "cloudhsm:DescribeClusters",
        "cloudtrail:GetDashboard",
        "cloudtrail:GetResourcePolicy",
        "cloudtrail:ListChannels",
        "cloudtrail:ListDashboards",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeInsightRules",
        "cloudwatch:ListAlarmMuteRules",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListManagedInsightRules",
        "cloudwatch:ListMetricStreams",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackageGroup",
        "codeartifact:DescribeRepository",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListAllowedRepositoriesForGroup",
        "codeartifact:ListDomains",
        "codeartifact:ListPackageGroups",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetFleets",
        "codebuild:ListFleets",
        "codebuild:ListProjects",
        "codecommit:ListRepositories",
        "codeconnections:GetConnection",
        "codeconnections:ListConnections",
        "codeconnections:ListHosts",
        "codedeploy:GetApplication",
        "codedeploy:GetDeploymentConfig",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentConfigs",
        "codedeploy:ListTagsForResource",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-profiler:ListTagsForResource",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
```

```
        "codeguru-reviewer:ListTagsForResource",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "codepipeline:ListWebhooks",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:GetSyncConfiguration",
        "codestar-connections:ListConnections",
        "codestar-connections:ListHosts",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListSyncConfigurations",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:AdminGetUser",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:DescribeManagedLoginBranding",
        "cognito-idp:DescribeTerms",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:GetLogDeliveryConfiguration",
        "cognito-idp:GetUICustomization",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListTerms",
        "cognito-idp:ListUserPools",
        "comprehend:DescribeDocumentClassifier",
        "comprehend:DescribeFlywheel",
        "comprehend:DescribeResourcePolicy",
        "comprehend:ListDocumentClassifiers",
        "comprehend:ListEntityRecognizers",
        "comprehend:ListFlywheels",
        "comprehend:ListTagsForResource",
        "config:DescribeConfigRules",
        "config:DescribeConformancePacks",
        "config:DescribeOrganizationConformancePacks",
        "config:GetStoredQuery",
        "config:ListStoredQueries",
        "config:ListTagsForResource",
        "connect-campaigns:DescribeCampaign",
        "connect-campaigns:ListCampaigns",
        "connect:DescribeAgentStatus",
        "connect:DescribeEmailAddress",
        "connect:DescribeEvaluationForm",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
```

```
        "connect:DescribePhoneNumber",
        "connect:DescribePredefinedAttribute",
        "connect:DescribePrompt",
        "connect:DescribeQuickConnect",
        "connect:DescribeRoutingProfile",
        "connect:DescribeRule",
        "connect:DescribeSecurityProfile",
        "connect:DescribeTrafficDistributionGroup",
        "connect:DescribeUser",
        "connect:DescribeUserHierarchyGroup",
        "connect:DescribeUserHierarchyStructure",
        "connect:DescribeView",
        "connect:GetTaskTemplate",
        "connect:ListAgentStatuses",
        "connect:ListApprovedOrigins",
        "connect:ListBots",
        "connect:ListEvaluationFormVersions",
        "connect:ListEvaluationForms",
        "connect:ListHoursOfOperations",
        "connect:ListInstanceAttributes",
        "connect:ListInstanceStorageConfigs",
        "connect:ListInstances",
        "connect:ListIntegrationAssociations",
        "connect:ListLambdaFunctions",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "connect:ListPredefinedAttributes",
        "connect:ListPrompts",
        "connect:ListQueueEmailAddresses",
        "connect:ListQueueQuickConnects",
        "connect:ListQueues",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileManualAssignmentQueues",
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListSecurityProfileApplications",
        "connect:ListSecurityProfileFlowModules",
        "connect:ListSecurityProfilePermissions",
        "connect:ListSecurityProfiles",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListTrafficDistributionGroups",
```

```
        "connect:ListUserHierarchyGroups",
        "connect:ListUsers",
        "connect:ListViewVersions",
        "connect:ListViews",
        "connect:SearchAvailablePhoneNumbers",
        "controltower:GetEnabledBaseline",
        "controltower:GetEnabledControl",
        "controltower:GetLandingZone",
        "controltower:ListEnabledBaselines",
        "controltower:ListEnabledControls",
        "controltower:ListLandingZones",
        "controltower:ListTagsForResource",
        "cur:DescribeReportDefinitions",
        "cur:ListTagsForResource",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:ListDataSets",
        "datapipeline:ListPipelines",
        "datasync:DescribeLocationAzureBlob",
        "datasync:DescribeLocationFsxOntap",
        "datasync:DescribeLocationFsxOpenZfs",
        "datasync:ListLocations",
        "datasync:ListTasks",
        "datazone:GetDataSource",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetGroupProfile",
        "datazone:GetSubscriptionTarget",
        "datazone:GetUserProfile",
        "datazone:ListDataSources",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListDomains",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentProfiles",
```

```
        "datazone:ListEnvironments",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListSubscriptionTargets",
        "datazone:SearchGroupProfiles",
        "datazone:SearchUserProfiles",
        "dax:DescribeClusters",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetLicenseEndpoint",
        "deadline:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetQueueLimitAssociation",
        "deadline:GetStorageProfile",
        "deadline:ListFarms",
        "deadline:ListFleets",
        "deadline:ListLicenseEndpoints",
        "deadline:ListMonitors",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListQueueLimitAssociations",
        "deadline:ListQueues",
        "deadline:ListStorageProfiles",
        "deadline:ListTagsForResource",
        "detective:GetMembers",
        "detective:ListGraphs",
        "detective:ListMembers",
        "detective:ListOrganizationAdminAccount",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTestGridProjects",
        "devops-guru:DescribeServiceIntegration",
        "devops-guru:ListNotificationChannels",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualInterfaces",
        "dlm:GetLifecyclePolicies",
        "dms:DescribeCertificates",
        "dms:DescribeDataMigrations",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationConfigs",
```

```
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTasks",
        "dms:ListDataProviders",
        "dms:ListInstanceProfiles",
        "dms:ListMigrationProjects",
        "dms:ListTagsForResource",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:ListTagsForResource",
        "ds:DescribeDirectories",
        "dsql:GetCluster",
        "dsql:GetClusterPolicy",
        "dsql:GetVpcEndpointServiceName",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:ListTables",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAwsNetworkPerformanceMetricSubscriptions",
        "ec2:DescribeCapacityReservationFleets",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeFpgaImages",
        "ec2:DescribeHostReservations",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeInstanceConnectEndpoints",
        "ec2:DescribeInstanceEventWindows",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamPools",
        "ec2:DescribeIpamResourceDiscoveries",
        "ec2:DescribeIpamResourceDiscoveryAssociations",
        "ec2:DescribeIpamScopes",
        "ec2:DescribeIpams",
```

```
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeTransitGatewayMeteringPolicies",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:DescribeTransitGatewayRouteTableAnnouncements",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVerifiedAccessEndpoints",
        "ec2:DescribeVerifiedAccessGroups",
        "ec2:DescribeVerifiedAccessInstanceLoggingConfigurations",
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessTrustProviders",
        "ec2:DescribeVolumes",
```

```
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcBlockPublicAccessExclusions",
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeVpcEncryptionControls",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetAllowedImagesSettings",
        "ec2:GetAssociatedEnclaveCertificateIamRoles",
        "ec2:GetRouteServerAssociations",
        "ec2:GetRouteServerPropagations",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetSubnetCidrReservations",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:SearchTransitGatewayRoutes",
        "ecr-public:DescribeRepositories",
        "ecr:DescribeRepositories",
        "ecr:DescribeRepositoryCreationTemplates",
        "ecr:GetRegistryScanningConfiguration",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeServices",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeCapability",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
```

```
        "eks:ListAddons",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListClusters",
        "eks:ListEksAnywhereSubscriptions",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeReservedCacheNodes",
        "elasticache:DescribeServerlessCaches",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeApplicationVersions",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeListenerAttributes",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTrustStoreRevocations",
        "elasticloadbalancing:DescribeTrustStores",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListSteps",
        "elemental-inference:GetFeed",
        "elemental-inference:ListFeeds",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:ListJobRuns",
        "emr-containers:ListJobTemplates",
```

```
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListSecurityConfigurations",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:ListApplications",
        "entityresolution:GetIdMappingWorkflow",
        "entityresolution:GetIdNamespace",
        "entityresolution:GetMatchingWorkflow",
        "entityresolution:GetPolicy",
        "entityresolution:GetSchemaMapping",
        "entityresolution:ListIdMappingWorkflows",
        "entityresolution:ListIdNamespaces",
        "entityresolution:ListMatchingWorkflows",
        "entityresolution:ListSchemaMappings",
        "entityresolution:ListTagsForResource",
        "es:GetApplication",
        "es:ListApplications",
        "es:ListDomainNames",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "finspace:ListEnvironments",
        "firehose:ListDeliveryStreams",
        "fis:GetTargetAccountConfiguration",
        "fis:ListExperimentTemplates",
        "fis:ListExperiments",
        "fis:ListTargetAccountConfigurations",
        "fms:ListPolicies",
        "fms:ListProtocolsLists",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasetImportJobs",
        "forecast:ListDatasets",
        "forecast:ListForecastExportJobs",
        "forecast:ListForecasts",
        "forecast:ListPredictorBacktestExportJobs",
        "forecast:ListPredictors",
        "frauddetector:GetDetectors",
```

```
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetVariables",
        "fsx:DescribeBackups",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "gamelift:DescribeContainerFleet",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeScalingPolicies",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListContainerFleets",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListLocations",
        "gamelift:ListScripts",
        "gameliftstreams:GetApplication",
        "gameliftstreams:GetStreamGroup",
        "gameliftstreams:ListApplications",
        "gameliftstreams:ListStreamGroups",
        "gameliftstreams:ListTagsForResource",
        "geo:DescribeKey",
        "geo:ListKeys",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListTrackers",
        "glacier:ListVaults",
        "globalaccelerator:DescribeCrossAccountAttachment",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCrossAccountAttachments",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "glue:GetBlueprint",
        "glue:GetCrawlers",
        "glue:GetDatabases",
        "glue:GetJobs",
        "glue:GetRegistry",
```

```
        "glue:GetSchemaVersion",
        "glue:GetSession",
        "glue:GetTables",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetTriggers",
        "glue:ListDataQualityRulesets",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "glue:ListSchemaVersions",
        "glue:ListSessions",
        "glue:ListTriggers",
        "glue:querySchemaVersionMetadata",
        "grafana:ListWorkspaces",
        "greengrass:GetDeployment",
        "greengrass:ListComponentVersions",
        "greengrass:ListComponents",
        "greengrass:ListConnectorDefinitions",
        "greengrass:ListCoreDefinitions",
        "greengrass:ListDeployments",
        "greengrass:ListDeviceDefinitions",
        "greengrass:ListFunctionDefinitions",
        "greengrass:ListGroups",
        "greengrass:ListLoggerDefinitions",
        "greengrass:ListResourceDefinitions",
        "greengrass:ListSubscriptionDefinitions",
        "groundstation:ListConfigs",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
        "guardduty:GetMalwareProtectionPlan",
        "guardduty:GetThreatEntitySet",
        "guardduty:GetTrustedEntitySet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListIPSets",
        "guardduty:ListMalwareProtectionPlans",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListThreatEntitySets",
        "guardduty:ListThreatIntelSets",
        "guardduty:ListTrustedEntitySets",
        "healthlake:GetDataTransformationProfile",
        "healthlake:ListFHIRDatastores",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
```

```
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListInstanceProfiles",
        "iam:ListMFADevices",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:GetWorkflow",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "imagebuilder:ListLifecyclePolicies",
        "imagebuilder:ListWorkflowBuildVersions",
        "imagebuilder:ListWorkflows",
        "inspector2:GetCodeSecurityScanConfiguration",
        "inspector2:ListCisScanConfigurations",
        "inspector2:ListCodeSecurityScanConfigurations",
        "inspector2:ListFilters",
        "inspector2:ListTagsForResource",
        "inspector:ListAssessmentTemplates",
        "internetmonitor:ListTagsForResource",
        "iot:DescribeCertificateProvider",
```

```
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:GetCommand",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetV2LoggingOptions",
        "iot:ListAuthorizers",
        "iot:ListBillingGroups",
        "iot:ListCACertificates",
        "iot:ListCertificateProviders",
        "iot:ListCertificates",
        "iot:ListCommands",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListJobs",
        "iot:ListMitigationActions",
        "iot:ListOTAUpdates",
        "iot:ListPackageVersions",
        "iot:ListPackages",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListStreams",
        "iot:ListThingGroups",
        "iot:ListThingTypes",
        "iot:ListThings",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListTunnels",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotdeviceadvisor:GetSuiteDefinition",
        "iotdeviceadvisor:ListSuiteDefinitions",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotfleethub:DescribeApplication",
        "iotfleethub:ListApplications",
```

```
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetStateTemplate",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListStateTemplates",
        "iotfleetwise:ListVehicles",
        "iotsitewise:DescribeComputationModel",
        "iotsitewise:DescribeDataset",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssets",
        "iotsitewise:ListComputationModels",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListDatasets",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjects",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:GetPartnerAccount",
        "iotwireless:GetWirelessDeviceImportTask",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListDevicesForWirelessDeviceImportTask",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListPartnerAccounts",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListWirelessDeviceImportTasks",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "iotwireless:ListWirelessGateways",
        "ivs:GetEncoderConfiguration",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetStage",
```

```
        "ivs:GetStorageConfiguration",
        "ivs:ListChannels",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource",
        "kafka:DescribeReplicator",
        "kafka:ListClusters",
        "kafka:ListConfigurations",
        "kafka:ListReplicators",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra-ranking:ListRescoreExecutionPlans",
        "kendra:ListAccessControlConfigurations",
        "kendra:ListDataSources",
        "kendra:ListExperiences",
        "kendra:ListFaqs",
        "kendra:ListFeaturedResultsSets",
        "kendra:ListIndices",
        "kendra:ListQuerySuggestionsBlockLists",
        "kendra:ListThesauri",
        "kinesis:ListStreams",
        "kinesisanalytics:ListApplications",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kms:ListKeys",
        "lakeformation:ListDataCellsFilter",
        "lambda:ListCapacityProviders",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "lambda:ListLayerVersions",
        "lambda:ListLayers",
        "lambda:ListVersionsByFunction",
        "launchwizard:ListDeploymentEvents",
```

```
        "launchwizard:ListDeployments",
        "launchwizard:ListTagsForResource",
        "lex:ListBotAliases",
        "lex:ListBots",
        "license-manager:ListDistributedGrants",
        "license-manager:ListTagsForResource",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDisks",
        "lightsail:GetInstanceSnapshot",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:ListTagsForResource",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutvision:ListProjects",
        "m2:ListEnvironments",
        "macie2:ListAllowLists",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindingsFilters",
        "macie2:ListMembers",
        "managedblockchain:ListAccessors",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGateways",
        "mediapackage-vod:ListAssets",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage:ListChannels",
        "mediapackage:ListOriginEndpoints",
        "mediastore:ListContainers",
        "mediatailor:ListChannels",
        "mediatailor:ListLiveSources",
        "mediatailor:ListPlaybackConfigurations",
        "mediatailor:ListSourceLocations",
        "mediatailor:ListVodSources",
        "memorydb:DescribeACLs",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeSnapshots",
        "memorydb:DescribeSubnetGroups",
```

```
        "memorydb:DescribeUsers",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTemplates",
        "mq:ListBrokers",
        "mq:ListConfigurations",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetDevices",
        "networkmanager:GetLinks",
        "networkmanager:ListAttachments",
        "networkmanager:ListCoreNetworks",
        "oam:ListSinks",
        "omics:ListReferenceStores",
        "omics:ListRunGroups",
        "omics:ListWorkflows",
        "organizations:DescribeResourcePolicy",
        "organizations:ListPolicies",
        "outposts:ListSites",
        "panorama:ListDevices",
        "panorama:ListPackages",
        "partnercentral:ListBenefitApplications",
        "partnercentral:ListEngagementInvitations",
        "partnercentral:ListEngagements",
        "partnercentral:ListOpportunities",
        "partnercentral:ListResourceSnapshotJobs",
        "partnercentral:ListResourceSnapshots",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "pipes:ListPipes",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentTemplates",
        "proton:ListServiceTemplates",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListLedgers",
        "quicksight:DescribeAccountSubscription",
```

```
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListFolders",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "ram:GetResourceShares",
        "ram:ListPermissions",
        "rbin:ListRules",
        "rbin:ListTagsForResource",
        "rds:DescribeBlueGreenDeployments",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeReservedDBInstances",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeHsmClientCertificates",
        "redshift:DescribeSnapshotCopyGrants",
        "redshift:DescribeSnapshotSchedules",
        "redshift:DescribeUsageLimits",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "rekognition:DescribeProjects",
        "rekognition:ListCollections",
        "resiliencehub:ListAppAssessments",
        "resiliencehub:ListApps",
```

```
        "resiliencehub:ListResiliencyPolicies",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListViews",
        "resource-groups:ListGroups",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53domains:ListDomains",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRules",
        "rum:ListAppMonitors",
        "s3:GetBucketLocation",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3express:ListAllMyDirectoryBuckets",
        "s3vectors:ListIndexes",
        "s3vectors:ListVectorBuckets",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListClusters",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListContexts",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
```

```
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHubContents",
        "sagemaker:ListHubs",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelCardVersions",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPartnerApps",
        "sagemaker:ListPipelines",
        "sagemaker:ListProjects",
        "sagemaker:ListSpaces",
        "sagemaker:ListStudioLifecycleConfigs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "scheduler:ListScheduleGroups",
        "schemas:ListDiscoverers",
        "secretsmanager:ListSecrets",
        "servicecatalog:ListApplications",
        "servicecatalog:ListAttributeGroups",
        "servicediscovery:ListServices",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListDedicatedIpPools",
        "ses:ListEmailIdentities",
        "ses:ListEmailTemplates",
        "shield:ListProtectionGroups",
        "shield:ListProtections",
```

```
        "signer:ListSigningProfiles",
        "sns:ListTopics",
        "sqs:ListQueues",
        "ssm-incidents:ListResponsePlans",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeMaintenanceWindowTargets",
        "ssm:DescribeMaintenanceWindowTasks",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeParameters",
        "ssm:DescribeSessions",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListResourceDataSync",
        "states:ListActivities",
        "states:ListStateMachines",
        "storagegateway:ListFileShares",
        "storagegateway:ListGateways",
        "swf:ListDomains",
        "synthetics:DescribeCanaries",
        "synthetics:ListGroups",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "verifiedpermissions:ListPolicyStores",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "wafv2:ListIPSets",
        "wafv2:ListRegexPatternSets",
        "wafv2:ListRuleGroups",
        "wafv2:ListWebACLs",
        "wellarchitected:ListWorkloads",
        "wisdom:ListAssistantAssociations",
        "wisdom:ListAssistants",
        "wisdom:ListContents",
```

```
        "wisdom:ListKnowledgeBases",
        "workspaces-web:ListPortals",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaces",
        "xray:GetSamplingRules"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PermissionsForReadGetResources",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListTagsForResource",
        "account-access:GetEntitlement",
        "account-access:ListEntitlements",
        "account:GetAlternateContact",
        "airflow:GetEnvironment",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListThemes",
        "app-integrations:ListEventIntegrationAssociations",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExperimentDefinition",
        "appconfig:GetExtensionAssociation",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListExperimentDefinitions",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:DescribeConnectorProfiles",
        "application-autoscaling:DescribeScalingPolicies",
        "apprunner:ListTagsForResource",
        "appstream:DescribeDirectoryConfigs",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "aps:DescribeWorkspace",
```

```
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "b2bi:GetTransformer",
        "b2bi:ListTransformers",
        "backup-gateway:ListVirtualMachines",
        "backup:DescribeBackupVault",
        "backup:DescribeFramework",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeReportPlan",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetTieringConfiguration",
        "backup:ListBackupSelections",
        "backup:ListFrameworks",
        "backup:ListTags",
        "backup:ListTieringConfigurations",
        "batch:DescribeSchedulingPolicies",
        "batch:ListTagsForResource",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetBrowserProfile",
        "bedrock-agentcore:GetPaymentCredentialProvider",
        "bedrock-agentcore:GetPolicyGenerationSummary",
        "bedrock-agentcore:ListBrowserProfiles",
        "bedrock-agentcore:ListPaymentCredentialProviders",
        "bedrock-agentcore:ListPolicyGenerationSummaries",
        "bedrock-agentcore:ListTagsForResource",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetFlowAlias",
```

```
        "bedrock:GetGuardrail",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetPromptRouter",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListTagsForResource",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListTagsForResource",
        "braket:ListTagsForResource",
        "braket:SearchSpendingLimits",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForBudget",
        "cases:BatchGetCaseRule",
        "cases:BatchGetField",
        "cases:GetDomain",
        "cases:GetLayout",
        "cases:GetTemplate",
        "cases:ListCaseRules",
        "cases:ListDomains",
        "cases:ListFields",
        "cases:ListLayouts",
        "cases:ListTemplates",
        "cassandra:Select",
        "chime:DescribeAppInstanceBot",
        "chime:DescribeAppInstanceUser",
        "chime:DescribeChannelFlow",
        "chime:ListChannelFlows",
        "cleanrooms-ml:ListConfiguredModelAlgorithms",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:ListMembers",
        "cleanrooms:ListTagsForResource",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:DescribeChangeSet",
        "cloudformation:GetResource",
```

```
        "cloudformation:ListChangeSets",
        "cloudformation:ListStackResources",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetFunction",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetChannel",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetAlarmMuteRule",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListTagsForResource",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codebuild:BatchGetReportGroups",
        "codebuild:ListReportGroups",
        "codebuild:ListSourceCredentials",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListTagsForResource",
        "codeconnections:ListTagsForResource",
        "codedeploy:GetDeployment",
        "codedeploy:GetDeploymentGroup",
        "codedeploy:ListDeploymentGroups",
        "codedeploy:ListDeployments",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codestar-connections:ListTagsForResource",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:ListGroups",
```

```
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserPoolClients",
        "config:DescribeAggregationAuthorizations",
        "connect:DescribeDataTable",
        "connect:DescribeHoursOfOperation",
        "connect:DescribeMetric",
        "connect:DescribeNotification",
        "connect:DescribeQueue",
        "connect:DescribeWorkspace",
        "connect:ListDataTables",
        "connect:ListHoursOfOperationOverrides",
        "connect:ListInstances",
        "connect:ListMetrics",
        "connect:ListNotifications",
        "connect:ListQuickConnects",
        "connect:ListSecurityProfileAIAgents",
        "connect:ListUserProficiencies",
        "connect:ListUsers",
        "connect:ListWorkspaceMedia",
        "connect:ListWorkspacePages",
        "connect:ListWorkspaces",
        "connect:SearchWorkspaceAssociations",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipeVersions",
        "databrew:ListSchedules",
        "databrew:ListTagsForResource",
        "dataexchange:GetRevision",
        "dataexchange:ListTagsForResource",
        "datasync:DescribeAgent",
        "datasync:DescribeLocationEfs",
        "datasync:DescribeLocationFsxLustre",
        "datasync:DescribeLocationFsxWindows",
        "datasync:DescribeLocationHdfs",
        "datasync:DescribeLocationNfs",
        "datasync:DescribeLocationS3",
```

```
        "datasync:DescribeLocationSmb",
        "datasync:DescribeTask",
        "datasync:ListAgents",
        "datasync:ListTagsForResource",
        "datasync:ListTasks",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "deadline:GetBudget",
        "deadline:GetJob",
        "deadline:ListBudgets",
        "deadline:ListJobs",
        "deadline:SearchJobs",
        "detective:DescribeOrganizationConfiguration",
        "detective:ListTagsForResource",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:ListNetworkProfiles",
        "devicefarm:ListTagsForResource",
        "devops-guru:GetResourceCollection",
        "directconnect:DescribeLags",
        "dlm:GetLifecyclePolicy",
        "dlm:ListTagsForResource",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "ds:DescribeDirectories",
        "ds:DescribeDomainControllers",
        "ds:DescribeEventTopics",
        "ds:ListLogSubscriptions",
        "ds:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeClientVpnTargetNetworks",
```

```
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeRouteServerEndpoints",
        "ec2:DescribeRouteServerPeers",
        "ec2:DescribeRouteServers",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeVolumeAttribute",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribePullThroughCacheRules",
        "ecr:DescribeRegistry",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListTagsForResource",
        "ecs:DescribeClusters",
        "ecs:DescribeExpressGatewayService",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTaskSets",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitionFamilies",
        "eks:DescribeCluster",
        "eks:ListCapabilities",
        "eks:ListTagsForResource",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:ListTagsForResource",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:DescribeTags",
```

```
        "elasticloadbalancing:DescribeCapacityReservation",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "elemental-inference:ListTagsForResource",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListJobRuns",
        "es:DescribeDomain",
        "es:DescribeDomains",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:GetCompatibleElasticsearchVersions",
        "es:GetCompatibleVersions",
        "es:ListDomainsForPackage",
        "es:ListTags",
        "es:ListVpcEndpointsForDomain",
        "events:DescribeApiDestination",
        "events:DescribeArchive",
        "events:DescribeConnection",
        "events:DescribeEndpoint",
        "events:DescribeEventBus",
        "events:DescribeRule",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "firehose:ListTagsForDeliveryStream",
        "fis:GetExperiment",
        "fis:GetExperimentTemplate",
```

```
        "fis:ListTagsForResource",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:ListTagsForResource",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:ListTagsForResource",
        "frauddetector:GetListElements",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeS3AccessPointAttachments",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "gamelift:DescribeAlias",
        "gamelift:DescribeBuild",
        "gamelift:DescribeContainerGroupDefinition",
        "gamelift:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListBuilds",
        "gamelift:ListContainerGroupDefinitions",
        "gamelift:ListLocations",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "gamelift:ValidateMatchmakingRuleSet",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeAcceleratorAttributes",
```

```
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:DescribeIntegrations",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetDatabase",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetWorkflow",
        "glue:ListBlueprints",
        "glue:ListCrawlers",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListTagsForResource",
        "greengrass:DescribeComponent",
        "greengrass:ListTagsForResource",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:ListConfigs",
        "groundstation:ListMissionProfiles",
        "groundstation:ListTagsForResource",
        "guardduty:DescribePublishingDestination",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
```

```
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:GetIPSet",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListFindings",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListTagsForResource",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:ListDataTransformationProfiles",
        "healthlake:ListTagsForResource",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:ListAttachedRolePolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfilesForRole",
        "iam:ListInstanceProfileTags",
        "iam:ListMFADeviceTags",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListMembers",
```

```
        "internetmonitor:GetMonitor",
        "internetmonitor:ListMonitors",
        "invoicing:ListProcurementPortalPreferences",
        "invoicing:ListTagsForResource",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeBillingGroup",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJob",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:DescribeStream",
        "iot:DescribeThing",
        "iot:GetPolicy",
        "iot:GetTopicRuleDestination",
        "iot:ListDomainConfigurations",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListV2LoggingLevels",
        "iot:ValidateSecurityProfileBehaviors",
        "iotfleetwise:GetCampaign",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:ListCampaigns",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListTagsForResource",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAssetModelCompositeModels",
```

```
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListTagsForResource",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:GetEntity",
        "iottwinmaker:GetScene",
        "iottwinmaker:GetSyncJob",
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListTagsForResource",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "ivs:GetComposition",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetRecordingConfiguration",
        "ivs:ListCompositions",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListTagsForResource",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:DescribeVpcConnection",
        "kafka:GetClusterPolicy",
        "kafka:ListClustersV2",
        "kafka:ListScramSecrets",
        "kafka:ListTagsForResource",
        "kafka:ListVpcConnections",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListTagsForResource",
```

```
        "kendra-ranking:DescribeRescoreExecutionPlan",
        "kendra-ranking:ListTagsForResource",
        "kendra:DescribeIndex",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:GetResourcePolicy",
        "kinesis:ListStreamConsumers",
        "kinesis:ListTagsForResource",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListResourceTags",
        "lakeformation:DescribeLakeFormationIdentityCenterConfiguration",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionScalingConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:ListAliases",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListFunctionUrlConfigs",
```

```
        "lambda:ListTags",
        "launchwizard:GetDeployment",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
        "lex:ListBotLocales",
        "lex:ListBotVersions",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListLicenses",
        "license-manager:ListReceivedGrants",
        "lightsail:GetActiveNames",
        "lightsail:GetDisk",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetInstance",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetLoadBalancers",
        "lightsail:GetOperations",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeAccountPolicies",
        "logs:DescribeDeliveries",
        "logs:DescribeDeliveryDestinations",
        "logs:DescribeDeliverySources",
        "logs:DescribeIndexPolicies",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeResourcePolicies",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
```

```
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetIntegration",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:ListIntegrations",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListTagsLogGroup",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:DescribeMetricSet",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:ListApplications",
        "m2:ListTagsForResource",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsFilter",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListAutomatedDiscoveryAccounts",
        "macie2:ListTagsForResource",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNodes",
        "mediaconnect:DescribeBridge",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeGateway",
        "mediaconnect:GetRouterInput",
        "mediaconnect:GetRouterNetworkInterface",
        "mediaconnect:ListBridges",
        "mediaconnect:ListRouterInputs",
        "mediaconnect:ListRouterNetworkInterfaces",
        "mediaconnect:ListRouterOutputs",
        "mediaconnect:ListTagsForResource",
        "medialive:DescribeChannelPlacementGroup",
```

```
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeNode",
        "medialive:DescribeSdiSource",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:ListChannelPlacementGroups",
        "medialive:ListCloudWatchAlarmTemplateGroups",
        "medialive:ListCloudWatchAlarmTemplates",
        "medialive:ListEventBridgeRuleTemplateGroups",
        "medialive:ListEventBridgeRuleTemplates",
        "medialive:ListMultiplexPrograms",
        "medialive:ListMultiplexes",
        "medialive:ListNodes",
        "medialive:ListSdiSources",
        "medialive:ListSignalMaps",
        "medialive:ListTagsForResource",
        "mediapackage-vod:DescribeAsset",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListTagsForResource",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediatailor:DescribeChannel",
        "mediatailor:DescribeLiveSource",
        "mediatailor:DescribeSourceLocation",
        "mediatailor:DescribeVodSource",
        "mediatailor:GetChannelPolicy",
        "mediatailor:GetPlaybackConfiguration",
        "medical-imaging:GetDatastore",
        "medical-imaging:ListDatastores",
        "medical-imaging:ListTagsForResource",
        "memorydb:DescribeParameters",
        "memorydb:ListTags",
        "mobiletargeting:GetApp",
```

```
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetCampaign",
        "mobiletargeting:GetEmailChannel",
        "mobiletargeting:GetEmailTemplate",
        "mobiletargeting:GetEventStream",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:GetSegment",
        "mobiletargeting:ListTagsForResource",
        "mpa:GetIdentitySource",
        "mpa:ListIdentitySources",
        "mpa:ListTagsForResource",
        "mq:DescribeBroker",
        "mq:DescribeConfiguration",
        "mq:ListTags",
        "neptune-graph:GetGraphSnapshot",
        "neptune-graph:GetPrivateGraphEndpoint",
        "neptune-graph:ListGraphSnapshots",
        "neptune-graph:ListPrivateGraphEndpoints",
        "neptune-graph:ListTagsForResource",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:DescribeVpcEndpointAssociation",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListTLSInspectionConfigurations",
        "network-firewall:ListVpcEndpointAssociations",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDirectConnectGatewayAttachment",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetSites",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
```

```
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:ListTagsForResource",
        "notifications:GetEventRule",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications:ListOrganizationalUnits",
        "notifications:ListTagsForResource",
        "nova-act:GetWorkflowDefinition",
        "nova-act:ListWorkflowDefinitions",
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListLinks",
        "oam:ListTagsForResource",
        "omics:GetAnnotationStore",
        "omics:GetConfiguration",
        "omics:GetReferenceStore",
        "omics:GetRun",
        "omics:GetRunCache",
        "omics:GetRunGroup",
        "omics:GetS3AccessPolicy",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:GetWorkflowVersion",
        "omics:ListAnnotationStores",
        "omics:ListConfigurations",
        "omics:ListRunCaches",
        "omics:ListRuns",
        "omics:ListSequenceStores",
        "omics:ListTagsForResource",
        "omics:ListVariantStores",
        "omics:ListWorkflowVersions",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
```

```
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "osis:GetPipeline",
        "osis:GetResourcePolicy",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "outposts:GetSite",
        "panorama:DescribeApplicationInstance",
        "panorama:DescribeDevice",
        "panorama:DescribePackageVersion",
        "panorama:ListApplicationInstances",
        "panorama:ListNodes",
        "panorama:ListTagsForResource",
        "partnercentral:GetBenefitApplication",
        "partnercentral:ListTagsForResource",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListServicePrincipalNames",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-ad:ListTemplateGroupAccessControlEntries",
        "pca-connector-ad:ListTemplates",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:ListChallengeMetadata",
        "pca-connector-scep:ListConnectors",
        "pca-connector-scep:ListTagsForResource",
        "pcs:GetCluster",
        "pcs:GetComputeNodeGroup",
        "pcs:GetQueue",
        "pcs:ListClusters",
        "pcs:ListComputeNodeGroups",
        "pcs:ListQueues",
        "pcs:ListTagsForResource",
        "personalize:DescribeDataset",
```

```
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetImportJobs",
        "personalize:ListTagsForResource",
        "pipes:DescribePipe",
        "profile:GetCalculatedAttributeDefinition",
        "profile:GetDomain",
        "profile:GetEventStream",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListCalculatedAttributeDefinitions",
        "profile:ListDomains",
        "profile:ListEventStreams",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "qbusiness:GetApplication",
        "qbusiness:GetDataSource",
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetPolicy",
        "qbusiness:GetRetriever",
        "qbusiness:GetWebExperience",
        "qbusiness:ListApplications",
        "qbusiness:ListDataSources",
        "qbusiness:ListIndices",
        "qbusiness:ListPlugins",
        "qbusiness:ListRetrievers",
        "qbusiness:ListTagsForResource",
        "qbusiness:ListWebExperiences",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeCustomPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeFolder",
        "quicksight:DescribeFolderPermissions",
        "quicksight:DescribeOAuthClientApplication",
        "quicksight:DescribeRefreshSchedule",
```

```
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:DescribeTopic",
        "quicksight:DescribeVPCConnection",
        "quicksight:ListAnalyses",
        "quicksight:ListCustomPermissions",
        "quicksight:ListDashboards",
        "quicksight:ListOAuthClientApplications",
        "quicksight:ListRefreshSchedules",
        "quicksight:ListTagsForResource",
        "quicksight:ListTopics",
        "quicksight:ListVPCConnections",
        "ram:GetPermission",
        "ram:GetResourceShareAssociations",
        "ram:ListPermissionAssociations",
        "ram:ListPermissionVersions",
        "ram:ListResources",
        "ram:ListResourceSharePermissions",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxyTargetGroups",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeIntegrations",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterDbRevisions",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeDataShares",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeIntegrations",
```

```
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeTags",
        "redshift:GetResourcePolicy",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetRoute",
        "refactor-spaces:GetService",
        "refactor-spaces:ListTagsForResource",
        "rekognition:DescribeCollection",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListTagsForResource",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListTagsForResource",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:ListGroupResources",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:ListTagsForResource",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53:GetChange",
        "route53:GetDNSSEC",
```

```
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListCidrBlocks",
        "route53:ListCidrCollections",
        "route53:ListCidrLocations",
        "route53:ListHostedZonesByName",
        "route53:ListQueryLoggingConfigs",
        "route53:ListResourceRecordSets",
        "route53:ListTagsForResource",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetOutpostResolver",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:ListFirewallDomains",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListOutpostResolvers",
        "route53resolver:ListResolverConfigs",
        "route53resolver:ListResolverDnssecConfigs",
        "route53resolver:ListResolverEndpointIpAddresses",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:ListResolverRuleAssociations",
        "route53resolver:ListTagsForResource",
        "rtbfabric:GetCertificateAssociation",
        "rtbfabric:GetInboundExternalLink",
        "rtbfabric:GetLink",
        "rtbfabric:GetLinkRoutingRule",
        "rtbfabric:GetOutboundExternalLink",
        "rtbfabric:GetRequesterGateway",
        "rtbfabric:GetResponderGateway",
        "rtbfabric:ListCertificateAssociations",
```

```
        "rtbfabric:ListLinkRoutingRules",
        "rtbfabric:ListLinks",
        "rtbfabric:ListRequesterGateways",
        "rtbfabric:ListResponderGateways",
        "rtbfabric:ListTagsForResource",
        "rum:GetAppMonitor",
        "rum:ListTagsForResource",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListRegionalBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
```

```
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsInstances",
        "s3:ListAccessGrantsLocations",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListTagsForResource",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
        "s3express:GetAccessPointScope",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetInventoryConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:GetMetricsConfiguration",
        "s3express:ListAccessPointsForDirectoryBuckets",
        "s3express:ListTagsForResource",
        "s3files:GetAccessPoint",
        "s3files:GetFileSystem",
        "s3files:GetFileSystemPolicy",
        "s3files:GetMountTarget",
        "s3files:GetSynchronizationConfiguration",
        "s3files:ListAccessPoints",
        "s3files:ListFileSystems",
        "s3files:ListMountTargets",
        "s3files:ListTagsForResource",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketMetricsConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableBucketReplication",
        "s3tables:GetTableBucketStorageClass",
        "s3tables:ListTableBuckets",
        "s3tables:ListTagsForResource",
```

```
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:ListTagsForResource",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeClusterSchedulerConfig",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeComputeQuota",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHub",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeMlflowApp",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelCardExportJob",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
```

```
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribeOptimizationJob",
        "sagemaker:DescribePartnerApp",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeStudioLifecycleConfig",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTrainingPlan",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListClusterSchedulerConfigs",
        "sagemaker:ListComputeQuotas",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListMlflowApps",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCardExportJobs",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListOptimizationJobs",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingPlans",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
```

```
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "sdb:GetAttributes",
        "sdb:ListDomains",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecretVersionIds",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetTargetDomains",
        "securityagent:GetApplication",
        "securityagent:ListApplications",
        "securityagent:ListPentests",
        "securityagent:ListTagsForResource",
        "securityagent:ListTargetDomains",
        "securityhub:DescribeHub",
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeStandardsControls",
        "securityhub:GetAggregatorV2",
        "securityhub:GetAutomationRuleV2",
        "securityhub:GetConfigurationPolicy",
        "securityhub:GetConfigurationPolicyAssociation",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindingAggregator",
        "securityhub:ListAggregatorsV2",
        "securityhub:ListAutomationRulesV2",
        "securityhub:ListConfigurationPolicies",
        "securityhub:ListConfigurationPolicyAssociations",
        "securityhub:ListEnabledProductsForImport",
        "securityhub:ListFindingAggregators",
        "securityhub:ListTagsForResource",
        "securitylake:GetSubscriber",
        "securitylake:ListDataLakeExceptions",
        "securitylake:ListDataLakes",
        "securitylake:ListLogSources",
        "securitylake:ListSubscribers",
        "securitylake:ListTagsForResource",
        "servicecatalog:DescribePortfolio",
        "servicecatalog:DescribePortfolioShares",
        "servicecatalog:DescribeProductAsAdmin",
        "servicecatalog:DescribeProvisionedProduct",
        "servicecatalog:DescribeProvisioningArtifact",
        "servicecatalog:DescribeServiceAction",
        "servicecatalog:DescribeTagOption",
```

```
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListPortfolios",
        "servicecatalog:ListProvisioningArtifacts",
        "servicecatalog:ListServiceActions",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:ListTagOptions",
        "servicecatalog:SearchProductsAsAdmin",
        "servicediscovery:GetInstance",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:ListInstances",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
        "ses:DescribeReceiptRuleSet",
        "ses:GetAddonInstance",
        "ses:GetAddonSubscription",
        "ses:GetAddressList",
        "ses:GetArchive",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailIdentity",
        "ses:GetEmailTemplate",
        "ses:GetIngressPoint",
        "ses:GetRelay",
        "ses:GetRuleSet",
        "ses:GetTemplate",
        "ses:GetTrafficPolicy",
        "ses:ListAddonInstances",
        "ses:ListAddonSubscriptions",
        "ses:ListAddressLists",
        "ses:ListArchives",
        "ses:ListIngressPoints",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListRelays",
        "ses:ListRuleSets",
        "ses:ListTagsForResource",
        "ses:ListTemplates",
```

```
        "ses:ListTrafficPolicies",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeProtectionGroup",
        "shield:DescribeSubscription",
        "shield:ListTagsForResource",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "simspaceweaver:DescribeSimulation",
        "simspaceweaver:ListSimulations",
        "sms-voice:DescribeConfigurationSets",
        "sms-voice:DescribeKeywords",
        "sms-voice:DescribeOptOutLists",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeProtectConfigurations",
        "sms-voice:DescribeSenderIds",
        "sms-voice:GetProtectConfigurationCountryRuleSet",
        "sms-voice:GetResourcePolicy",
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "sns:GetDataProtectionPolicy",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:GetRotation",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListRotations",
        "ssm-contacts:ListTagsForResource",
        "ssm-guiconnect:GetConnectionRecordingPreferences",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListTagsForResource",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:ListConfigurationManagers",
```

```
        "ssm-sap:GetApplication",
        "ssm-sap:ListApplications",
        "ssm-sap:ListTagsForResource",
        "ssm:DescribeAssociation",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
        "ssm:DescribePatchBaselines",
        "ssm:GetAutomationExecution",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetMaintenanceWindow",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:GetServiceSetting",
        "ssm:ListTagsForResource",
        "sso:DescribeApplication",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetPermissionsBoundaryForPermissionSet",
        "sso:ListApplications",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
        "states:DescribeStateMachineAlias",
        "states:ListStateMachineAliases",
        "states:ListStateMachineVersions",
        "states:ListTagsForResource",
        "storagegateway:ListTagsForResource",
        "storagegateway:ListVolumes",
        "sts:GetCallerIdentity",
        "support:DescribeCases",
        "supportapp:ListSlackChannelConfigurations",
        "supportapp:ListSlackWorkspaceConfigurations",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
```

```
        "synthetics:ListGroupResources",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "textract:GetAdapter",
        "textract:ListAdapters",
        "textract:ListTagsForResource",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:ListTagsForResource",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeScheduledQuery",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListScheduledQueries",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transcribe:GetCallAnalyticsJob",
        "transcribe:GetVocabularyFilter",
        "transcribe:ListCallAnalyticsJobs",
        "transcribe:ListTagsForResource",
        "transcribe:ListVocabularyFilters",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWebApp",
        "transfer:DescribeWebAppCustomization",
        "transfer:DescribeWorkflow",
        "transfer:ListTagsForResource",
        "transfer:ListWebApps",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicyTemplates",
        "verifiedpermissions:ListTagsForResource",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetListener",
```

```
        "vpc-lattice:GetResourceConfiguration",
        "vpc-lattice:GetResourceGateway",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkResourceAssociation",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListResourceConfigurations",
        "vpc-lattice:ListResourceGateways",
        "vpc-lattice:ListServiceNetworkResourceAssociations",
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListTargets",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:GetWebACL",
        "waf-regional:GetWebACLForResource",
        "waf-regional:ListLoggingConfigurations",
        "waf:GetLoggingConfiguration",
        "waf:GetWebACL",
        "wafv2:GetIPSet",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRegexPatternSet",
        "wafv2:GetRuleGroup",
        "wafv2:GetWebACL",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListTagsForResource",
        "wisdom:GetAIAgent",
        "wisdom:GetAIGuardrail",
        "wisdom:GetAIPrompt",
        "wisdom:GetAssistant",
        "wisdom:ListAIAgentVersions",
        "wisdom:ListAIAgents",
        "wisdom:ListAIGuardrails",
        "wisdom:ListAIGuardrailVersions",
        "wisdom:ListAIPrompts",
        "wisdom:ListAIPromptVersions",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
```

```
        "workspaces-web:ListIpAccessSettings",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListUserSettings",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspacesPools",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetIndexingRules",
        "xray:GetTraceSegmentDestination",
        "xray:ListResourcePolicies",
        "xray:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSResourceGroupsReadOnlyAccess

Deskripsi: Ini adalah kebijakan baca saja untuk Grup AWS Sumber Daya

`AWSResourceGroupsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSResourceGroupsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 07 Maret 2018, 10:27 UTC
- Waktu teredit: 05 Februari 2019, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "tag:Get*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcs",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeSnapshots",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListClusters",
        "glacier:ListVaults",
        "glacier:DescribeVault",
        "glacier:ListTagsForVault",
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
```

```
        "kinesis:ListTagsForStream",
        "opsworks:DescribeStacks",
        "opsworks:ListTags",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters",
        "redshift:DescribeTags",
        "route53domains:ListDomains",
        "route53:ListHealthChecks",
        "route53:GetHealthCheck",
        "route53:ListHostedZones",
        "route53:GetHostedZone",
        "route53:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListTagsForResource",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "ssm:ListDocuments"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSRevenueAttributionManagement

Deskripsi: Menyediakan akses yang diperlukan untuk kegiatan manajemen atribusi pendapatan.

`AWSRevenueAttributionManagement`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSRevenueAttributionManagement` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Juni 2026, 16:57 UTC
- Waktu teredit: 30 Juni 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRevenueAttributionManagement`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RevenueAttributionCreation",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateRevenueAttribution"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "RevenueAttributionListing",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListRevenueAttributions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "RevenueAttributionManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetRevenueAttribution",
        "partnercentral:UpdateRevenueAttribution"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/revenue-attribution/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "TaggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:TagResource",
        "partnercentral:UntagResource",
        "partnercentral:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/revenue-attribution/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSRoboMaker_FullAccess

Deskripsi: Menyediakan akses penuh ke AWS RoboMaker melalui Konsol Manajemen AWS dan SDK. Juga menyediakan akses tertentu ke layanan terkait (misalnya, S3, IAM).

`AWSRoboMaker_FullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSRoboMaker_FullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 September 2020, 18:34 UTC
- Waktu teredit: 16 September 2021, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "robomaker:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecr:BatchGetImage",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecr-public:DescribeImages",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:CalledViaFirst" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "robomaker.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSRoboMakerReadOnlyAccess

Deskripsi: Menyediakan akses baca saja AWS RoboMaker melalui Konsol Manajemen AWS dan SDK

`AWSRoboMakerReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSRoboMakerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 26 November 2018, 05:30 UTC
- Waktu teredit: 28 Agustus 2020, 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSRoboMakerServicePolicy

Deskripsi: kebijakan RoboMaker layanan

`AWSRoboMakerServicePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 26 November 2018, 06:30 UTC
- Waktu teredit: 11 November 2021, 22:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "greengrass:CreateDeployment",
```

```
        "greengrass:CreateGroupVersion",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetAssociatedRole",
        "lambda:CreateFunction",
        "robomaker:CreateSimulationJob",
        "robomaker:CancelSimulationJob"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "robomaker:TagResource"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:robomaker:*:*:simulation-job/*"
    },
    {
      "Action" : [
        "lambda:UpdateFunctionCode",
        "lambda:GetFunction",
        "lambda:UpdateFunctionConfiguration",
        "lambda:DeleteFunction",
        "lambda:ListVersionsByFunction",
        "lambda:GetAlias",
        "lambda:UpdateAlias",
        "lambda:CreateAlias",
        "lambda:DeleteAlias"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:lambda:*:*:function:aws-robomaker-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "robomaker.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSRoboMakerServiceRolePolicy

Deskripsi: kebijakan RoboMaker layanan

`AWSRoboMakerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSRoboMakerServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 November 2018, 05:33 UTC
- Waktu teredit: 26 November 2018, 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "greengrass:CreateDeployment",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetAssociatedRole",
        "lambda:CreateFunction"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "lambda:UpdateFunctionCode",
        "lambda:GetFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:lambda:*:*:function:aws-robomaker-*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSRolesAnywhereFullAccess

Deskripsi: Menyediakan semua izin ke sumber daya IAM Roles Anywhere, termasuk namun tidak terbatas pada: CreateProfile,, Disable DeleteTrustAnchor CRL,. ResetNotificationSettings

`AWSRolesAnywhereFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSRolesAnywhereFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 Juli 2025, 14:52 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRolesAnywhereFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustAnchors",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListTrustAnchors",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:CreateTrustAnchor",
        "rolesanywhere:DeleteTrustAnchor",
        "rolesanywhere:DisableTrustAnchor",
        "rolesanywhere:EnableTrustAnchor",
        "rolesanywhere:UpdateTrustAnchor"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:trust-anchor/*"
      ]
    },
    {
      "Sid" : "Profiles",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListProfiles",
        "rolesanywhere:GetProfile",
        "rolesanywhere:CreateProfile",
        "rolesanywhere:DeleteProfile",
        "rolesanywhere:DisableProfile",
        "rolesanywhere:EnableProfile",
        "rolesanywhere:UpdateProfile"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:profile/*"
```

```
      ]
    },
    {
      "Sid" : "CRLs",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListCrls",
        "rolesanywhere:GetCrl",
        "rolesanywhere:DeleteCrl",
        "rolesanywhere:DisableCrl",
        "rolesanywhere:EnableCrl",
        "rolesanywhere:ImportCrl",
        "rolesanywhere:UpdateCrl"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:crl/*"
      ]
    },
    {
      "Sid" : "Subjects",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListSubjects",
        "rolesanywhere:GetSubject"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:subject/*"
      ]
    },
    {
      "Sid" : "OtherRolesAnywherePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:PutAttributeMapping",
        "rolesanywhere:DeleteAttributeMapping",
        "rolesanywhere:ResetNotificationSettings",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:TagResource",
        "rolesanywhere:UntagResource",
        "rolesanywhere:PutNotificationSettings"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "PassRoleToRolesAnywhere",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "rolesanywhere.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateRolesAnywhereServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "rolesanywhere.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSRolesAnywhereReadOnly

Deskripsi: Menyediakan izin baca-saja ke sumber daya IAM Roles Anywhere, termasuk namun tidak terbatas pada: GetTrustAnchor,, ListProfiles GetCRL. Tidak akan ada izin lain untuk layanan lain yang termasuk dalam kebijakan ini.

`AWSRolesAnywhereReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSRolesAnywhereReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 Juli 2025, 15:07 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRolesAnywhereReadOnly`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Profiles",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListProfiles",
        "rolesanywhere:GetProfile"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:profile/*"
      ]
    },
    {
      "Sid" : "CRLs",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListCrls",
```

```
        "rolesanywhere:GetCrl"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:crl/*"
      ]
    },
    {
      "Sid" : "Subjects",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListSubjects",
        "rolesanywhere:GetSubject"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:subject/*"
      ]
    },
    {
      "Sid" : "TrustAnchors",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListTrustAnchors",
        "rolesanywhere:GetTrustAnchor"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:trust-anchor/*"
      ]
    },
    {
      "Sid" : "Tags",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSRolesAnywhereServicePolicy

Deskripsi: Mengizinkan IAM Roles Anywhere menerbitkan service/usage metrik ke CloudWatch dan memeriksa status Otoritas Sertifikat Pribadi atas nama Anda.

`AWSRolesAnywhereServicePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 05 Juli 2022, 15:26 UTC
- Waktu teredit: 05 Juli 2022, 15:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/RolesAnywhere",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSS3OnOutpostsServiceRolePolicy

Deskripsi: Izinkan layanan Amazon S3 di Outposts untuk mengelola sumber daya jaringan EC2 atas nama Anda.

`AWSS3OnOutpostsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 03 Oktober 2023, 20:32 UTC
- Waktu teredit: 03 Oktober 2023, 20:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSS3OnOutpostsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2:DescribeAddresses",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations"
      ],
```

```
      "Resource" : "*",
      "Sid" : "DescribeVpcResources"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Sid" : "CreateNetworkInterface"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "S3 On Outposts"
        }
      },
      "Sid" : "CreateTagsForCreateNetworkInterface"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:ipv4pool-ec2/*"
      ],
      "Sid" : "AllocateIpAddress"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "S3 On Outposts"
        }
      },
      "Sid" : "CreateTagsForAllocateIpAddress"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:AssociateAddress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "S3 On Outposts"
        }
      },
      "Sid" : "ReleaseVpcResources"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface",
            "AllocateAddress"
          ],
          "aws:RequestTag/CreatedBy" : [
            "S3 On Outposts"
          ]
```

```
        }
      },
      "Sid" : "CreateTags"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSavingsPlansFullAccess

Deskripsi: Menyediakan akses penuh ke layanan Paket Tabungan

`AWSSavingsPlansFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSavingsPlansFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 November 2019, 22:45 UTC
- Waktu teredit: 06 November 2019, 22.45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "savingsplans:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSavingsPlansReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke layanan Paket Tabungan

`AWSSavingsPlansReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSavingsPlansReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 November 2019, 22:45 UTC
- Waktu teredit: 06 November 2019, 22.45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "savingsplans:Describe*",
        "savingsplans:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSDMPServiceRolePolicy

Deskripsi: Izinkan SDMP membuat dan mengelola sumber daya atas nama pelanggan.

`AWSSDMPServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 24 Juli 2026, 20:57 UTC
- Waktu teredit: 10 Agustus 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSDMPServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:GetServiceLinkedChannel",
        "cloudtrail:UpdateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/sdmp/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "AllowListOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListServiceLinkedChannels",
        "iam:ListPolicies",
        "iam:ListPolicyTags",
        "iam:ListRoles",
        "account:ListRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateRoleWithConditions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:PutRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/SDMP-*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/AWSDenyAll"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aws:ResourceTag/CreatedBy" : "arn:aws:iam::*:role/SDMPServiceRole*"
        }
      }
    },
    {
      "Sid" : "AllowSDMPRoleTagging",
      "Effect" : "Allow",
      "Action" : "iam:TagRole",
      "Resource" : "arn:aws:iam::*:role/SDMP-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "CreatedBy"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AttachAWSDenyAll",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Resource" : "arn:aws:iam::*:role/SDMP-*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/AWSDenyAll"
        },
        "StringLike" : {
          "aws:ResourceTag/CreatedBy" : "arn:aws:iam::*:role/SDMPServiceRole*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReadSDMPRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListRoleTags",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/SDMP-*",
        "arn:aws:iam::*:role/SDMPServiceRole*",
        "arn:aws:iam::*:role/aws-service-role/sdmp.amazonaws.com/AWSServiceRoleForSDMP"
      ]
    },
    {
      "Sid" : "ReadSDMPPolicies",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListPolicyVersions"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:policy/SDMP*"
      ]
    },
    {
      "Sid" : "AllowSecurityServiceVerification",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:ListDetectors",
        "guardduty:GetDetector",
        "macie2:GetMacieSession",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "securityhub:DescribeHub",
        "securityhub:ListFindingAggregators",
        "inspector2:BatchGetAccountStatus",
        "detective:ListGraphs",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSecretsManagerClientReadOnlyAccess

Deskripsi: Menyediakan akses untuk mengambil dan menjelaskan rahasia dari Manajer Rahasia. Kebijakan ini juga memungkinkan dekripsi kunci KMS untuk rahasia Manajer Rahasia.

`AWSSecretsManagerClientReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSecretsManagerClientReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 November 2025, 20:04 UTC
- Waktu teredit: 02 Juni 2026, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecretsManagerClientReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecretsManagerGetAndDescribeSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*"
    },
    {
      "Sid" : "SecretsManagerBatchGetSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:BatchGetSecretValue",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSDecryptKey",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:*:*:secret:*",
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSecurityAgentServiceRolePolicy

Deskripsi: Men AWS gizinkan Agen Keamanan mengelola sumber daya atas nama Anda.

`AWSSecurityAgentServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 11 Juni 2026, 23:42 UTC
- Waktu teredit: 11 Juni 2026, 23:42 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityAgentServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LatticeCreateResourceGateway",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:CreateResourceGateway"
      ],
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSSecurityAgentManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LatticeTagResourceGateway",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:TagResource"
      ],
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSSecurityAgentManaged" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "LatticeManageTaggedResourceGateways",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:DeleteResourceGateway"
      ],
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSSecurityAgentManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LatticeGetResourceGateway",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:GetResourceGateway"
      ],
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSSecurityAgentManaged" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeApis",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateLatticeServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice",
      "Condition" : {
        "StringLike" : {
```

```
          "iam:AWSServiceName" : "vpc-lattice.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSecurityAgentWebAppPolicy

Deskripsi: Memberikan izin bagi pengguna yang diautentikasi untuk mengakses Aplikasi Web Agen Keamanan untuk mengonfigurasi dan menjalankan pengujian penetrasi keamanan otomatis. Kebijakan ini memungkinkan pengguna mengelola pentest, melihat temuan, memantau eksekusi pengujian, dan berinteraksi dengan AWS sumber daya yang diperlukan untuk operasi pengujian keamanan.

`AWSSecurityAgentWebAppPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSecurityAgentWebAppPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Februari 2026, 23:19 UTC
- Waktu teredit: 24 September 2026, 23:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSSecurityAgentWebAppPolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:ListAgentSpaces",
        "securityagent:ListSecurityRequirements",
        "securityagent:ListTargetDomains",
        "securityagent:BatchGetTargetDomains"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AgentSpaceAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:AddArtifact",
        "securityagent:CreateThreat",
        "securityagent:BatchDeleteCodeReviews",
        "securityagent:BatchDeletePentests",
        "securityagent:BatchDeleteThreatModels",
        "securityagent:BatchGetAgentSpaces",
        "securityagent:BatchGetArtifactMetadata",
        "securityagent:BatchGetCodeReviewJobs",
        "securityagent:BatchGetCodeReviewJobTasks",
        "securityagent:BatchGetCodeReviews",
        "securityagent:BatchGetFindings",
        "securityagent:BatchGetPentestJobContentMetadata",
        "securityagent:BatchGetPentestJobs",
        "securityagent:BatchGetPentestJobTasks",
```

```
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetThreatModelJobs",
        "securityagent:BatchGetThreatModelJobTasks",
        "securityagent:BatchGetThreatModels",
        "securityagent:BatchGetThreats",
        "securityagent:BatchGetValidationRuns",
        "securityagent:CreateCodeReview",
        "securityagent:CreateDesignReview",
        "securityagent:CreatePentest",
        "securityagent:CreateThreatModel",
        "securityagent:DeleteArtifact",
        "securityagent:DeleteDesignReview",
        "securityagent:GetArtifact",
        "securityagent:GetDesignReview",
        "securityagent:GetDesignReviewArtifact",
        "securityagent:GetDesignReviewFeedback",
        "securityagent:ListActorMessages",
        "securityagent:ListArtifacts",
        "securityagent:ListCodeReviewJobsForCodeReview",
        "securityagent:ListCodeReviewJobTasks",
        "securityagent:ListCodeReviews",
        "securityagent:ListDesignReviewComments",
        "securityagent:ListDesignReviews",
        "securityagent:ListDiscoveredDomains",
        "securityagent:ListDiscoveredEndpoints",
        "securityagent:ListFindings",
        "securityagent:ListIntegratedResources",
        "securityagent:ListPentestJobsForPentest",
        "securityagent:ListPentestJobTasks",
        "securityagent:ListPentests",
        "securityagent:ListThreatModelJobs",
        "securityagent:ListThreatModelJobTasks",
        "securityagent:ListThreatModels",
        "securityagent:ListThreats",
        "securityagent:PutDesignReviewFeedback",
        "securityagent:StartCodeRemediation",
        "securityagent:StartCodeReviewJob",
        "securityagent:StartPentestJob",
        "securityagent:StartThreatModelJob",
        "securityagent:StartValidationRun",
        "securityagent:StopCodeReviewJob",
        "securityagent:StopPentestJob",
        "securityagent:StopThreatModelJob",
        "securityagent:UpdateCodeReview",
```

```
        "securityagent:UpdateDiscoveredDomains",
        "securityagent:UpdateFinding",
        "securityagent:UpdatePentest",
        "securityagent:UpdateThreat",
        "securityagent:UpdateThreatModel"
      ],
      "Resource" : "arn:aws:securityagent:*:*:agent-space*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSecurityHubFullAccess

Deskripsi: Menyediakan akses penuh untuk menggunakan Hub AWS Keamanan.

`AWSSecurityHubFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSecurityHubFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2018, 23:54 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC

- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubFullAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubAllowAll",
      "Effect" : "Allow",
      "Action" : "securityhub:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "securityhub.amazonaws.com",
            "securityhubv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OtherServicePermission",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:GetDetector",
        "guardduty:ListDetectors",
        "guardduty:UpdateDetector",
```

```
        "guardduty:EnableOrganizationAdminAccount",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:DeleteDetector",
        "guardduty:CreateDetector",
        "guardduty:CreateMembers",
        "guardduty:UpdateOrganizationConfiguration",
        "guardduty:DescribeOrganizationConfiguration",
        "inspector2:BatchGetAccountStatus",
        "inspector2:Enable",
        "inspector2:Disable",
        "inspector2:EnableDelegatedAdminAccount",
        "inspector2:DisableDelegatedAdminAccount",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:UpdateOrganizationConfiguration",
        "inspector2:DescribeOrganizationConfiguration",
        "pricing:GetProducts",
        "account:ListRegions",
        "account:GetRegionOptStatus",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSecurityHubOrganizationsAccess

Deskripsi: Memberikan izin untuk mengaktifkan dan mengelola Hub AWS Keamanan dalam organisasi. Termasuk mengaktifkan layanan di seluruh organisasi, dan menentukan akun administrator yang didelegasikan untuk layanan.

`AWSSecurityHubOrganizationsAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSecurityHubOrganizationsAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Maret 2021, 20:53 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubOrganizationsAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:DescribeAccount",
```

```
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:DescribeResourcePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationPermissionsEnable",
      "Effect" : "Allow",
      "Action" : "organizations:EnableAWSServiceAccess",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com",
            "inspector2.amazonaws.com",
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationPermissionsDelegatedAdmin",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:account/o-*/*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com",
            "inspector2.amazonaws.com",
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "OrganizationPolicyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:EnablePolicyType",
        "organizations:DisablePolicyType"
      ],
      "Resource" : [
        "arn:aws:organizations::*:root/o-*/*",
        "arn:aws:organizations::*:account/o-*/*",
        "arn:aws:organizations::*:ou/o-*/*",
        "arn:aws:organizations::*:policy/o-*/securityhub_policy/*",
        "arn:aws:organizations::*:policy/o-*/inspector_policy/*"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:PolicyType" : [
            "SECURITYHUB_POLICY",
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationPolicyTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:TagResource",
        "organizations:UntagResource",
        "organizations:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:organizations::*:policy/o-*/securityhub_policy/*",
        "arn:aws:organizations::*:policy/o-*/inspector_policy/*"
      ]
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSecurityHubReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke sumber daya Hub AWS Keamanan

`AWSSecurityHubReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSecurityHubReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2018, 01:34 UTC
- Waktu teredit: 22 Februari 2024, 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSecurityHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:Get*",
        "securityhub:List*",
        "securityhub:BatchGet*",
        "securityhub:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSecurityHubServiceRolePolicy

Deskripsi: Peran terkait layanan diperlukan untuk Hub AWS Keamanan untuk mengakses sumber daya Anda.

`AWSSecurityHubServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 27 November 2018, 23:47 UTC

- Waktu teredit: 27 Juni 2026, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v16 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubServiceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "logs:DescribeMetricFilters",
        "sns:ListSubscriptionsByTopic",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRules",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:BatchGetResourceConfig",
        "config:SelectResourceConfig",
        "iam:GenerateCredentialReport",
        "organizations:ListAccounts",
        "config:PutEvaluations",
        "tag:GetResources",
        "iam:GetCredentialReport",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
```

```
        "organizations:ListChildren",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "securityhub:BatchDisableStandards",
        "securityhub:BatchEnableStandards",
        "securityhub:BatchUpdateStandardsControlAssociations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:CreateMembers",
        "securityhub:DeleteMembers",
        "securityhub:DescribeHub",
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeStandards",
        "securityhub:DescribeStandardsControls",
        "securityhub:DisassociateFromAdministratorAccount",
        "securityhub:DisassociateMembers",
        "securityhub:DisableSecurityHub",
        "securityhub:EnableSecurityHub",
        "securityhub:GetEnabledStandards",
        "securityhub:ListStandardsControlAssociations",
        "securityhub:ListSecurityControlDefinitions",
        "securityhub:UpdateOrganizationConfiguration",
        "securityhub:UpdateSecurityControl",
        "securityhub:UpdateSecurityHubConfiguration",
        "securityhub:UpdateStandardsControl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubServiceRoleConfigPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule",
        "config:DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/*securityhub*"
    },
    {
      "Sid" : "SecurityHubServiceRoleOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecurityHubCSPMServiceRoleConfig",
      "Effect" : "Allow",
      "Action" : [
        "config:PutServiceLinkedConfigurationRecorder",
        "config:PutThirdPartyServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : [
        "arn:aws:config:*:*:configuration-recorder/
*ConfigurationRecorderForSecurityHubCSPM*"
      ]
    },
    {
      "Sid" : "SecurityHubCSPMServiceRoleConfigListAndGet",
      "Effect" : "Allow",
      "Action" : [
        "config:ListConfigurationRecorders",
        "config:GetConnector"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubCSPMServiceRoleIamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "SecurityHubCSPMServiceRoleConfigMetricsPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSecurityHubV2ServiceRolePolicy

Deskripsi: Kebijakan ini memungkinkan Hub Keamanan mengelola aturan AWS konfigurasi dan sumber daya Hub Keamanan di organisasi Anda dan atas nama Anda.

`AWSSecurityHubV2ServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 10 Juni 2025, 17:37 UTC
- Waktu teredit: 27 Juni 2026, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubV2ServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubV2ServiceRoleAssetsConfig",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:PutServiceLinkedConfigurationRecorder",
        "config:PutThirdPartyServiceLinkedConfigurationRecorder"
      ],
      "Resource" : "arn:aws:config:*:*:configuration-recorder/
*ConfigurationRecorderForSecurityHubAssets*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleAssetsConfigListAndGet",
      "Effect" : "Allow",
      "Action" : [
        "config:ListConfigurationRecorders",
        "config:GetConnector"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleAssetsIamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleSecurityHubPermissions",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:DisableSecurityHubV2",
        "securityhub:EnableSecurityHubV2",
        "securityhub:DescribeSecurityHubV2",
        "securityhub:EnableSecurityHubFeatureV2",
        "securityhub:DisableSecurityHubFeatureV2"
      ],
      "Resource" : "arn:aws:securityhub:*:*:hubv2/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleOrganizationsPermissionsOnResources",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "arn:aws:organizations::*:*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleOrganizationsPermissionsWithoutResources",
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleDelegatedAdminPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleEcrListingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeImages",
        "ecr:DescribeRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleLambdaAndConfigMetricPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleLambdaListingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleIamListingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetAccountSummary"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleIA2IamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/access-analyzer.amazonaws.com/
AWSServiceRoleForAccessAnalyzer"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "access-analyzer.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleIA2ResAPermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CreateServiceLinkedAnalyzer",
        "access-analyzer:DeleteServiceLinkedAnalyzer"
      ],
      "Resource" : "arn:*:access-analyzer:*:*:analyzer/*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleIA2ResAListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ListAnalyzers"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleIA2APIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetFindingRecommendation",
        "access-analyzer:GenerateFindingRecommendation"
      ],
      "Resource" : "arn:*:access-analyzer:*:*:analyzer/
_AccessAnalyzerForSecurityHubV2*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleAPIPolicyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",
        "iam:GetUserPolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*",
        "arn:aws:iam::*:user/*"
      ]
    },
    {
      "Sid" : "SecurityHubConnectorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:CreateConnector",
        "securityhub:UpdateConnector",
        "securityhub:DeleteConnector"
      ],
      "Resource" : "arn:aws:securityhub:*:*:connector/*",
      "Condition" : {
        "StringLikeIfExists" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "SecurityHubV2ServiceRoleInspectorConnectorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:CreateConnector",
        "inspector2:DeleteConnector",
        "inspector2:ListConnectors",
        "inspector2:ListConnectorScanConfigurations",
        "inspector2:UpdateConnector",
        "inspector2:UpdateConnectorScanConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleInspectorIamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
thirdparty.inspector2.amazonaws.com/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "thirdparty.inspector2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleOutboundIdentityFederationPermission",
      "Effect" : "Allow",
      "Action" : "sts:GetWebIdentityToken",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "sts:IdentityTokenAudience" : [
            "api://AzureADTokenExchange"
          ]
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSecurityIncidentResponseCaseFullAccess

Deskripsi: Kebijakan memberi pelanggan izin Baca dan Tulis ke sumber daya kasus yang dibuat melalui layanan Respon Insiden Keamanan.

`AWSSecurityIncidentResponseCaseFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSecurityIncidentResponseCaseFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2024, 23:21 UTC
- Waktu teredit: 22 April 2026, 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityIncidentResponseCaseFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIRCaseFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:GetCase",
        "security-ir:ListCases",
        "security-ir:GetCaseAttachmentDownloadUrl",
        "security-ir:ListComments",
        "security-ir:ListCaseEdits",
        "security-ir:CreateCase",
        "security-ir:UpdateCase",
        "security-ir:CloseCase",
        "security-ir:UpdateCaseStatus",
        "security-ir:UpdateResolverType",
        "security-ir:GetCaseAttachmentUploadUrl",
        "security-ir:CreateCaseComment",
        "security-ir:UpdateCaseComment",
        "security-ir:SendFeedback",
        "security-ir:ListInvestigations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityIRCaseTagFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:ListTagsForResource",
        "security-ir:TagResource",
        "security-ir:UntagResource"
      ],
      "Resource" : "arn:aws:security-ir:*:*:case/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSecurityIncidentResponseFullAccess

Deskripsi: Kebijakan memberi pelanggan izin Baca dan Tulis ke semua sumber daya yang terkait dengan layanan Respon Insiden Keamanan.

`AWSSecurityIncidentResponseFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSecurityIncidentResponseFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2024, 23:21 UTC
- Waktu teredit: 22 April 2026, 16:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityIncidentResponseFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIRFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:*"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoleForSecurityIncidentResponse",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/security-ir.amazonaws.com/
AWSServiceRoleForSecurityIncidentResponse"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "security-ir.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoleForSecurityIncidentResponseTriage",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/triage.security-ir.amazonaws.com/
AWSServiceRoleForSecurityIncidentResponse_Triage"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "triage.security-ir.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OrganizationsPolicies",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
```

```
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSecurityIncidentResponseReadOnlyAccess

Deskripsi: Kebijakan memberikan Read-only izin kepada pelanggan ke semua sumber daya yang terkait dengan layanan Respon Insiden Keamanan. Izin mencakup akses ke GetCaseAttachmentDownloadUrl juga untuk kemampuan untuk mendapatkan URL unduhan lampiran kasus.

`AWSSecurityIncidentResponseReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSecurityIncidentResponseReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2024, 23:06 UTC
- Waktu teredit: 01 Oktober 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityIncidentResponseReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIRReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:BatchGetMemberAccountDetails",
        "security-ir:GetMembership",
        "security-ir:ListMemberships",
        "security-ir:GetCase",
        "security-ir:ListCases",
        "security-ir:GetCaseAttachmentDownloadUrl",
        "security-ir:ListComments",
        "security-ir:ListCaseEdits",
        "security-ir:ListTagsForResource",
        "security-ir:ListInvestigations",
        "security-ir:GetFindingMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSecurityIncidentResponseServiceRolePolicy

Deskripsi: Menyediakan akses ke AWS Sumber Daya yang dikelola atau digunakan oleh Respon Insiden Keamanan

`AWSSecurityIncidentResponseServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 01 Desember 2024, 16:36 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityIncidentResponseServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIncidentResponseOrganizationsPolicy",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
```

```
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityIncidentResponseCreateCasePolicyTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:TagResource",
        "security-ir:CreateCase"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SecurityIncidentResponseManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SecurityIncidentResponseManaged" : "true",
          "aws:ResourceTag/SecurityIncidentResponseManaged" : "true"
        }
      },
      "Resource" : "arn:aws:security-ir:*:*:case/*"
    },
    {
      "Sid" : "SecurityIncidentResponseOperationsPolicy",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:GetCase",
        "security-ir:UpdateCase",
        "security-ir:ListCases",
        "security-ir:CreateCaseComment",
        "security-ir:ListComments"
      ],
      "Resource" : "arn:aws:security-ir:*:*:case/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSecurityIncidentResponseTriageServiceRolePolicy

Deskripsi: Menyediakan akses ke Respon Insiden AWS Keamanan untuk terus memantau lingkungan Anda untuk ancaman keamanan, menyetel layanan keamanan untuk mengurangi kebisingan peringatan, dan mengumpulkan informasi untuk menyelidiki potensi insiden.

`AWSSecurityIncidentResponseTriageServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 01 Desember 2024, 16:36 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityIncidentResponseTriageServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "triage.security-ir.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:ArchiveFindings",
        "guardduty:CreateFilter",
        "guardduty:DescribeMalwareScans",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:StartMalwareScan",
        "guardduty:UpdateFindingsFeedback"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "securityhub:BatchUpdateFindings",
        "securityhub:DescribeHub",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindings",
        "securityhub:ListEnabledProductsForImport",
        "securityhub:UpdateFindings"
      ],
      "Resource" : "arn:aws:securityhub:*:*:hub/default"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "security-ir:CreateCase",
        "security-ir:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SecurityIncidentResponseManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SecurityIncidentResponseManaged" : "true",
          "aws:ResourceTag/SecurityIncidentResponseManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "security-ir:UpdateCase"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SecurityIncidentResponseManaged" : "true"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "security-ir:GetMembership",
        "security-ir:ListMemberships"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceCatalogAdminFullAccess

Deskripsi: Menyediakan akses penuh ke kemampuan admin katalog layanan

`AWSServiceCatalogAdminFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSServiceCatalogAdminFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Februari 2018, 17:19 UTC
- Waktu teredit: 04 Agustus 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListStackResources",
        "cloudformation:TagResource",
        "cloudformation:UntagResource",
        "cloudformation:CreateStackSet",
        "cloudformation:CreateStackInstances",
        "cloudformation:UpdateStackSet",
        "cloudformation:UpdateStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
```

```
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateUploadBucket",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ValidateTemplate",
        "iam:GetGroup",
        "iam:GetRole",
        "iam:GetUser",
        "iam:ListGroups",
        "iam:ListRoles",
        "iam:ListUsers",
        "servicecatalog:Get*",
        "servicecatalog:Scan*",
        "servicecatalog:Search*",
        "servicecatalog:List*",
        "servicecatalog:TagResource",
        "servicecatalog:UntagResource",
        "servicecatalog:SyncResource",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:ListDocumentVersions",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:Accept*",
        "servicecatalog:Associate*",
        "servicecatalog:Batch*",
        "servicecatalog:Copy*",
        "servicecatalog:Create*",
        "servicecatalog:Delete*",
        "servicecatalog:Describe*",
        "servicecatalog:Disable*",
        "servicecatalog:Disassociate*",
        "servicecatalog:Enable*",
```

```
        "servicecatalog:Execute*",
        "servicecatalog:Import*",
        "servicecatalog:Provision*",
        "servicecatalog:Put*",
        "servicecatalog:Reject*",
        "servicecatalog:Terminate*",
        "servicecatalog:Update*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "servicecatalog.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
orgsdatasync.servicecatalog.amazonaws.com/AWSServiceRoleForServiceCatalogOrgsDataSync",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "orgsdatasync.servicecatalog.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceCatalogAdminReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke kemampuan admin Katalog Layanan

`AWSServiceCatalogAdminReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSServiceCatalogAdminReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Oktober 2019, 18:53 UTC
- Waktu teredit: 25 Oktober 2019, 18.53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStackSet",
```

```
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "iam:GetGroup",
        "iam:GetRole",
        "iam:GetUser",
        "iam:ListGroups",
        "iam:ListRoles",
        "iam:ListUsers",
        "servicecatalog:Get*",
        "servicecatalog:List*",
        "servicecatalog:Describe*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:Search*",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:ListDocumentVersions",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceCatalogAppRegistryFullAccess

Deskripsi: Menyediakan akses penuh ke kemampuan Service Catalog App Registry

`AWSServiceCatalogAppRegistryFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSServiceCatalogAppRegistryFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 November 2020, 22:25 UTC
- Waktu teredit: 12 Agustus 2026, 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AppRegistryUpdateStackAndResourceGroupTagging",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:UpdateStack",
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "servicecatalog-appregistry.amazonaws.com"
        },
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "UpdateStack"
          ]
        }
      }
    },
    {
      "Sid" : "AppRegistryResourceGroupsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "resource-groups:GetGroup",
        "resource-groups:GetTags",
        "resource-groups:Tag",
        "resource-groups:Untag",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:AssociateResource",
        "resource-groups:DisassociateResource"
      ],
```

```
      "Resource" : "arn:aws:resource-groups:*:*:group/AWS_*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AppRegistryServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/servicecatalog-
appregistry.amazonaws.com/AWSServiceRoleForAWSServiceCatalogAppRegistry*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AppRegistryOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "servicecatalog:CreateApplication",
        "servicecatalog:GetApplication",
        "servicecatalog:UpdateApplication",
        "servicecatalog:DeleteApplication",
        "servicecatalog:ListApplications",
        "servicecatalog:AssociateResource",
        "servicecatalog:DisassociateResource",
        "servicecatalog:GetAssociatedResource",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup",
        "servicecatalog:ListAssociatedAttributeGroups",
        "servicecatalog:CreateAttributeGroup",
        "servicecatalog:UpdateAttributeGroup",
        "servicecatalog:DeleteAttributeGroup",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:SyncResource",
        "servicecatalog:ListAttributeGroupsForApplication",
        "servicecatalog:GetConfiguration",
```

```
        "servicecatalog:PutConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AppRegistryResourceTagging",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListTagsForResource",
        "servicecatalog:UntagResource",
        "servicecatalog:TagResource"
      ],
      "Resource" : "arn:aws:servicecatalog:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceCatalogAppRegistryReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke kemampuan Registri Aplikasi Katalog Layanan

`AWSServiceCatalogAppRegistryReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSServiceCatalogAppRegistryReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 November 2020, 22:34 UTC

- Waktu teredit: 17 November 2022 18.16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:GetApplication",
        "servicecatalog:ListApplications",
        "servicecatalog:GetAssociatedResource",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListAssociatedAttributeGroups",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:ListTagsForResource",
        "servicecatalog:ListAttributeGroupsForApplication",
        "servicecatalog:GetConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceCatalogAppRegistryServiceRolePolicy

Deskripsi: Mengizinkan Katalog Layanan AppRegistry untuk mengelola Grup Sumber Daya atas nama Anda

`AWSServiceCatalogAppRegistryServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 18 Mei 2021, 22:18 UTC
- Waktu teredit: 26 Oktober 2022, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:DescribeStacks",
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:DeleteGroup",
        "resource-groups:UpdateGroup",
        "resource-groups:GetTags",
        "resource-groups:Tag",
        "resource-groups:Untag"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration"
      ],
      "Resource" : [
        "arn:*:resource-groups:*:*:group/AWS_AppRegistry*",
        "arn:*:resource-groups:*:*:group/AWS_CloudFormation_Stack*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceCatalogEndUserFullAccess

Deskripsi: Menyediakan akses penuh ke kapabilitas pengguna akhir katalog layanan

`AWSServiceCatalogEndUserFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSServiceCatalogEndUserFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Februari 2018, 17:22 UTC
- Waktu teredit: 04 Agustus 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:SetStackPolicy",
        "cloudformation:ValidateTemplate",
        "cloudformation:UpdateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DeleteChangeSet",
        "cloudformation:TagResource",
        "cloudformation:UntagResource",
        "cloudformation:CreateStackSet",
        "cloudformation:CreateStackInstances",
        "cloudformation:UpdateStackSet",
        "cloudformation:UpdateStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListLaunchPaths",
```

```
        "servicecatalog:ProvisionProduct",
        "servicecatalog:SearchProducts",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:DescribeProvisionedProduct",
        "servicecatalog:DescribeRecord",
        "servicecatalog:ListRecordHistory",
        "servicecatalog:ListStackInstancesForProvisionedProduct",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:CreateProvisionedProductPlan",
        "servicecatalog:DescribeProvisionedProductPlan",
        "servicecatalog:ExecuteProvisionedProductPlan",
        "servicecatalog:DeleteProvisionedProductPlan",
        "servicecatalog:ListProvisionedProductPlans",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:ExecuteProvisionedProductServiceAction",
        "servicecatalog:DescribeServiceActionExecutionParameters"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceCatalogEndUserReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke kemampuan pengguna akhir Katalog Layanan

`AWSServiceCatalogEndUserReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSServiceCatalogEndUserReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Oktober 2019, 18:49 UTC
- Waktu teredit: 25 Oktober 2019, 18.49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
```

```
        "cloudformation:DescribeChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListLaunchPaths",
        "servicecatalog:SearchProducts",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:DescribeProvisionedProduct",
        "servicecatalog:DescribeRecord",
        "servicecatalog:ListRecordHistory",
        "servicecatalog:ListStackInstancesForProvisionedProduct",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:DescribeProvisionedProductPlan",
        "servicecatalog:ListProvisionedProductPlans",
```

```
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:DescribeServiceActionExecutionParameters"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceCatalogOrgsDataSyncServiceRolePolicy

Deskripsi: Kebijakan Peran Terkait Layanan AWS ServiceCatalog untuk disinkronkan dengan struktur AWS organisasi Organisasi

`AWSServiceCatalogOrgsDataSyncServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 10 April 2023, 20:48 UTC
- Waktu teredit: 08 Desember 2025, 19:04 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalogRegions",
      "Effect" : "Allow",
      "Action" : [
        "account:ListRegions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceCatalogSyncServiceRolePolicy

Deskripsi: Peran Tertaut Layanan AWS ServiceCatalog untuk menyinkronkan Artefak Penyediaan dari repositori sumber

`AWSServiceCatalogSyncServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 15 November 2022, 21:20 UTC
- Waktu teredit: 03 Mei 2024, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListProvisioningArtifacts",
        "servicecatalog:DescribeProductAsAdmin",
        "servicecatalog:DeleteProvisioningArtifact",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:DescribeProvisioningArtifact",
        "servicecatalog:CreateProvisioningArtifact",
        "servicecatalog:UpdateProvisioningArtifact"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessArtifactRepositories",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "ValidateTemplate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRoleForAIDevOpsPolicy

Deskripsi: Peran Tertaut Layanan ini menyediakan AIDevOps kemampuan untuk memberikan informasi penggunaan.

`AWSServiceRoleForAIDevOpsPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 16 Februari 2026, 14:27 UTC
- Waktu teredit: 27 Maret 2026, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAIDevOpsPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/AIDevOps"
          ]
        }
      }
    },
    {
      "Sid" : "LatticeCreateResourceGateway",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:CreateResourceGateway"
      ],
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSAIDevOpsManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LatticeTagResourceGateway",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:TagResource"
      ],
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSAIDevOpsManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LatticeManageTaggedResourceGateways",
      "Effect" : "Allow",
```

```
      "Action" : [
        "vpc-lattice:DeleteResourceGateway"
      ],
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSAIDevOpsManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LatticeGetResourceGateway",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:GetResourceGateway"
      ],
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSAIDevOpsManaged" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeApis",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateLatticeServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "vpc-lattice.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRoleForAmazonEKSNodegroup

Deskripsi: Izin diperlukan untuk mengelola grup simpul di akun pelanggan. Kebijakan ini terkait dengan pengelolaan sumber daya berikut: AutoscalingGroups, SecurityGroups, LaunchTemplates dan InstanceProfiles.

`AWSServiceRoleForAmazonEKSNodegroup`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 07 November 2019, 01:34 UTC
- Waktu teredit: 17 Februari 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SharedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks" : "*"
        }
      }
    },
    {
      "Sid" : "EKSCreatedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "LaunchTemplateRelatedPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "AutoscalingRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:PutLifecycleHook",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:EnableMetricsCollection",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:PutWarmPool",
        "autoscaling:DeleteWarmPool"
      ],
      "Resource" : "arn:aws:autoscaling:*:*:*:autoScalingGroupName/eks-*"
    },
    {
      "Sid" : "AllowAutoscalingToCreateSLR",
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "autoscaling.amazonaws.com"
        }
      },
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowASGCreationByEKS",
```

```
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:CreateAutoScalingGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToAutoscaling",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsToManageResourcesForNodegroups",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:GetRole",
        "ec2:CreateLaunchTemplate",
        "ec2:DescribeInstances",
        "iam:GetInstanceProfile",
        "ec2:DescribeLaunchTemplates",
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:RunInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:GetConsoleOutput",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeCapacityReservations",
        "autoscaling:DescribeWarmPool"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PermissionsToCreateAndManageInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks-*"
    },
    {
      "Sid" : "PermissionsToDeleteEKSAndKubernetesTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name",
            "kubernetes.io/cluster/*"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "PermissionsForManagedNodegroupsAutoRepair",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "PermissionsToCreateEKSAndKubernetesTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:security-group/*",
        "arn:*:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "AllowTaggingEC2ResourcesOnlyDuringInstanceCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
```

```
        "arn:*:ec2:*:*:instance/*",
        "arn:*:ec2:*:*:volume/*",
        "arn:*:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        },
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRoleForAmazonQDeveloper

Deskripsi: Peran Tertaut Layanan ini menyediakan kemampuan Amazon Q Developer untuk memberikan informasi penggunaan.

`AWSServiceRoleForAmazonQDeveloper`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 25 April 2024, 07:40 UTC
- Waktu teredit: 20 Juli 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonQDeveloper`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Q"
          ]
        }
      }
    },
    {
      "Sid" : "sid2",
      "Effect" : "Allow",
```

```
      "Action" : [
        "identitystore:ListGroupMembershipsForMember"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRoleForAWSTransform

Deskripsi: Service-Linked Peran ini menyediakan AWS Transform dengan kemampuan untuk memberikan informasi penggunaan.

`AWSServiceRoleForAWSTransform`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 15 Mei 2025, 13:37 UTC
- Waktu teredit: 12 Februari 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAWSTransform`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PublishCloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Transform"
          ]
        }
      }
    },
    {
      "Sid" : "UserManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeApplication",
        "sso:GetApplicationAssignmentConfiguration",
        "sso:ListApplicationAssignmentsForPrincipal"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SupportCaseManagement",
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:AddCommunicationToCase",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ExternalIdpSecretsAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
```

```
      "Resource" : "arn:aws:secretsmanager:*:*:secret:transform!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "transform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRoleForAWSTransformCustom

Deskripsi: Mengizinkan AWS Transform Custom untuk menerbitkan CloudWatch metrik ke akun Anda atas nama Anda.

`AWSServiceRoleForAWSTransformCustom`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 25 Maret 2026, 02:57 UTC
- Waktu teredit: 05 Mei 2026, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAWSTransformCustom`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/TransformCustom"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/TransformCustom",
        "arn:aws:logs:*:*:log-group:/aws/TransformCustom:log-stream:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

Deskripsi: Menyediakan akses ke sumber daya Manajer Sistem yang digunakan oleh CloudWatch Alarm

`AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 01 Oktober 2020, 09:49 UTC
- Waktu teredit: 01 Oktober 2020, 09:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePoli

Deskripsi: Memungkinkan CloudWatch untuk mengakses metrik RDS Performance Insights atas nama Anda

`AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 07 September 2023, 09:32 UTC
- Waktu teredit: 07 September 2023, 09:32 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRoleForCodeGuru-Profiler

Deskripsi: Peran terkait layanan yang diperlukan agar Amazon CodeGuru Profiler mengirim pemberitahuan atas nama Anda.

`AWSServiceRoleForCodeGuru-Profiler`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 26 Juni 2020, 22:04 UTC
- Waktu teredit: 26 Juni 2020, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuru-Profiler`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSNSPublishToSendNotifications",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sns:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRoleForCodeWhispererPolicy

Deskripsi: Peran ini memberikan izin CodeWhisperer untuk mengakses data di akun Anda untuk menghitung penagihan, menyediakan akses untuk membuat dan mengakses laporan keamanan di Amazon CodeGuru, dan mengirimkan data ke CloudWatch.

`AWSServiceRoleForCodeWhispererPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 24 Maret 2023, 19:39 UTC
- Waktu teredit: 09 April 2026, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid2",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListProfileAssociations",
        "sso:ListProfiles",
        "sso:ListDirectoryAssociations",
        "sso:DescribeRegisteredRegions",
        "sso:GetProfile",
        "sso:GetManagedApplicationInstance",
        "sso:ListApplicationAssignments",
        "sso:DescribeInstance",
        "sso:DescribeApplication"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid3",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateUploadUrl"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid4",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateScan",
        "codeguru-security:GetScan",
        "codeguru-security:ListFindings",
        "codeguru-security:GetFindings"
      ],
      "Resource" : [
        "arn:aws:codeguru-security:*:*:scans/CodeWhisperer-*"
      ]
    },
    {
      "Sid" : "sid5",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/CodeWhisperer"
          ]
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
```

```
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRoleForEC2ScheduledInstances

Deskripsi: Mengizinkan Instans Terjadwal EC2 untuk meluncurkan dan mengelola instans spot.

`AWSServiceRoleForEC2ScheduledInstances`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 12 Oktober 2017, 18:31 UTC
- Waktu teredit: 12 Oktober 2017, 18:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:ec2sri:scheduledInstanceId"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2sri:scheduledInstanceId" : "*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

Deskripsi: AWS GroundStation menggunakan peran terkait layanan ini untuk memanggil EC2 untuk menemukan alamat IPv4 publik

`AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 13 Desember 2022, 23:52 UTC
- Waktu teredit: 13 Desember 2022, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRoleForImageBuilder

Deskripsi: Memungkinkan EC2ImageBuilder untuk menelepon AWS layanan atas nama Anda.

`AWSServiceRoleForImageBuilder`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 29 November 2019, 22:02 UTC
- Waktu teredit: 09 Juli 2026, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForImageBuilder`

Versi kebijakan

Versi kebijakan: v28 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:RegisterImage",
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RegisterImage",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "vmie.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:CreateImage",
        "ec2:CreateLaunchTemplate",
        "ec2:DeregisterImage",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:ModifyImageAttribute",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeSnapshots",
        "ec2:DescribeHosts"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateImage"
          ],
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:export-image-task/*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "license-manager:UpdateLicenseSpecificationsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:ListCommandInvocations",
        "ssm:AddTagsToResource",
        "ssm:DescribeInstanceInformation",
        "ssm:GetAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:ListInventoryEntries",
        "ssm:SendAutomationSignal",
        "ssm:DescribeInstanceAssociationsStatus",
        "ssm:DescribeAssociationExecutions",
```

```
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunPowerShellScript",
        "arn:aws:ssm:*:*:document/AWS-RunShellScript",
        "arn:aws:ssm:*:*:document/AWSEC2-RunSysprep",
        "arn:aws:s3:::*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/CreatedBy" : [
            "EC2 Image Builder"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:EncryptionContextKeys" : [
            "aws:ebs:id"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
```

```
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/EC2ImageBuilderDistributionCrossAccountRole"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DescribeLaunchTemplates",
        "ec2:ModifyLaunchTemplate",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ExportImage"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:ExportImage"
      ],
      "Resource" : "arn:aws:ec2:*:*:export-image-task/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelExportTask"
      ],
      "Resource" : "arn:aws:ec2:*:*:export-image-task/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ssm.amazonaws.com",
            "ec2fastlaunch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableFastLaunch"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachImageWatermark"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector2:ListCoverage",
        "inspector2:ListFindings"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:TagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/image-builder-*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchDeleteImage"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/image-builder-*",
      "Condition" : {
        "StringEquals" : {
          "ecr:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/ImageBuilder-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/imagebuilder/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "imagebuilder:StartImagePipelineExecution",
```

```
      "Resource" : "arn:aws:imagebuilder:*:*:image-pipeline/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "imagebuilder:TagResource",
      "Resource" : "arn:aws:imagebuilder:*:*:image-pipeline/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRoleForIoTSiteWise

Deskripsi: AWS Memungkinkan IoT SiteWise untuk menyediakan dan mengelola gateway serta data kueri. Kebijakan ini mencakup izin AWS Greengrass yang diperlukan untuk penerapan ke grup, izin AWS Lambda untuk membuat dan memperbarui fungsi awalan layanan, dan izin AWS IoT Analytics untuk menanyakan data dari penyimpanan data.

`AWSServiceRoleForIoTSiteWise`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 14 November 2018, 19:19 UTC
- Waktu teredit: 13 November 2023, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSiteWiseReadGreenGrass",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:GetAssociatedRole",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSiteWiseAccessLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
```

```
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*"
    },
    {
      "Sid" : "AllowSiteWiseAccessLog",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*:log-stream:*"
    },
    {
      "Sid" : "AllowSiteWiseAccessSiteWiseManagedWorkspaceInTwinMaker",
      "Effect" : "Allow",
      "Action" : [
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ExecuteQuery"
      ],
      "Resource" : "arn:aws:iottwinmaker:*:*:workspace/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iottwinmaker:linkedServices" : [
            "IOTSITEWISE"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRoleForLogDeliveryPolicy

Deskripsi: Mengizinkan layanan Pengiriman Log mengirimkan log dengan memanggil tujuan log atas nama Anda.

`AWSServiceRoleForLogDeliveryPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 04 Oktober 2019, 17:31 UTC
- Waktu yang diedit: 15 Mei 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LogDeliveryToFirehose",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:ListTagsForDeliveryStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LogDeliveryEnabled" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "KMSForFirehoseSSECMK",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "firehose.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRoleForMonitronPolicy

Deskripsi: Memberikan izin Amazon Monitron untuk mengelola AWS sumber daya, termasuk penugasan pengguna AWS SSO atas nama Anda.

`AWSServiceRoleForMonitronPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran

- Waktu pembuatan: 02 Desember 2020, 19:06 UTC
- Waktu teredit: 07 Januari 2026, 09:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso:GetProfile",
        "sso:ListProfiles",
        "sso:ListProfileAssociations",
        "sso:AssociateProfile",
        "sso:ListDirectoryAssociations",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "sso:CreateApplicationAssignment",
        "sso:ListApplicationAssignments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRoleForNeptuneGraphPolicy

Deskripsi: Menyediakan akses Cloudwatch untuk mempublikasikan metrik dan log operasional dan penggunaan untuk Amazon Neptune

`AWSServiceRoleForNeptuneGraphPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 29 November 2023, 14:03 UTC
- Waktu teredit: 29 November 2023, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GraphMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Neptune",
            "AWS/Usage"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "GraphLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/neptune/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GraphLogEvents",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRoleForPrivateMarketplaceAdminPolicy

Deskripsi: Memberikan izin untuk menjelaskan dan memperbarui sumber daya Pasar Pribadi dan menjelaskan AWS Organisasi

`AWSServiceRoleForPrivateMarketplaceAdminPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 14 Februari 2024, 22:28 UTC
- Waktu teredit: 14 Februari 2024, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForPrivateMarketplaceAdminPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrivateMarketplaceCatalogDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
```

```
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Audience/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProcurementPolicy/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/BrandingSettings/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceCatalogDescribeChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceCatalogListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceStartChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : [
            "AssociateAudience",
            "DisassociateAudience"
          ]
        }
      },
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceOrganizationPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListChildren"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRoleForProcurementInsightsPolicy

Deskripsi: Kebijakan untuk Wawasan Pengadaan untuk mendapatkan rincian Akun Organisasi

`AWSServiceRoleForProcurementInsightsPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 03 Oktober 2024, 14:26 UTC
- Waktu teredit: 03 Oktober 2024, 14:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForProcurementInsightsPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProcurementInsightsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRoleForSMS

Deskripsi: Menyediakan akses ke AWS layanan dan sumber daya yang diperlukan untuk memigrasikan instans layanan ke AWS termasuk EC2, S3, dan Cloudformation.

`AWSServiceRoleForSMS`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 06 Agustus 2019, 18:39 UTC
- Waktu teredit: 15 Oktober 2020, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*",
      "Condition" : {
        "Null" : {
          "cloudformation:ResourceTypes" : "false"
        },
        "ForAllValues:StringEquals" : {
          "cloudformation:ResourceTypes" : [
            "AWS::EC2::Instance",
            "AWS::ApplicationInsights::Application",
```

```
            "AWS::ResourceGroups::Group"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplate"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::sms-app-*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "sms:CreateReplicationJob",
        "sms:DeleteReplicationJob",
        "sms:GetReplicationJobs",
        "sms:GetReplicationRuns",
        "sms:GetServers",
        "sms:ImportServerCatalog",
        "sms:StartOnDemandReplicationRun",
        "sms:UpdateReplicationJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunRemoteScript",
        "arn:aws:s3:::sms-app-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/UseForSMSApplicationValidation" : [
            "true"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CopySnapshot"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CopySnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SMSJobId" : [
            "sms-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/SMSJobId" : [
            "sms-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DeregisterImage",
```

```
        "ec2:ImportImage",
        "ec2:DescribeImportImageTasks",
        "ec2:GetEbsEncryptionByDefault"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetInstanceProfile"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "cloudformation.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute",
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:Describe*",
        "applicationinsights:List*",
```

```
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:CreateApplication",
        "applicationinsights:CreateComponent",
        "applicationinsights:UpdateApplication",
        "applicationinsights:DeleteApplication",
        "applicationinsights:UpdateComponentConfiguration",
        "applicationinsights:DeleteComponent"
      ],
      "Resource" : "arn:aws:applicationinsights:*:*:application/resource-group/sms-app-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:GetGroup",
        "resource-groups:UpdateGroup",
        "resource-groups:DeleteGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/sms-app-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:AWSServiceName" : "application-insights.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRoleForUserSubscriptions

Deskripsi: Menyediakan akses ke layanan Pengguna Langganan ke sumber daya Pusat Identitas Anda untuk memperbarui langganan Anda secara otomatis.

`AWSServiceRoleForUserSubscriptions`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 25 April 2024, 16:14 UTC
- Waktu teredit: 22 Juni 2026, 08:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForUserSubscriptions`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SubscriptionManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "organizations:DescribeOrganization",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:ListInstances",
        "sso-directory:DescribeUser",
        "sso:ListApplicationAssignments"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRolePolicyForBackupReports

Deskripsi: Men AWS yediakan izin Cadangan untuk membuat laporan kepatuhan atas nama Anda

`AWSServiceRolePolicyForBackupReports`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran

- Waktu pembuatan: 19 Agustus 2021, 21:16 UTC
- Waktu teredit: 10 Maret 2023, 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeFramework",
        "backup:ListBackupJobs",
        "backup:ListRestoreJobs",
        "backup:ListCopyJobs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:BatchGetResourceConfig",
        "config:SelectResourceConfig",
        "config:DescribeConfigurationAggregators",
        "config:SelectAggregateResourceConfig",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:DescribeConfigRules",
        "s3:GetBucketLocation"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:GetComplianceDetailsByConfigRule",
        "config:PutConfigRule",
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/
backup.amazonaws.com*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigurationAggregator",
        "config:PutConfigurationAggregator"
      ],
      "Resource" : "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
backup.amazonaws.com*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRolePolicyForBackupRestoreTesting

Deskripsi: Kebijakan ini berisi izin untuk pengujian pemulihan dan untuk membersihkan sumber daya yang dibuat selama pengujian.

`AWSServiceRolePolicyForBackupRestoreTesting`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 10 November 2023, 23:37 UTC
- Waktu teredit: 25 September 2026, 01:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BackupActions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeRecoveryPoint",
        "backup:DescribeRestoreJob",
        "backup:DescribeProtectedResource",
        "backup:GetRecoveryPointRestoreMetadata",
        "backup:ListBackupVaults",
        "backup:ListProtectedResources",
        "backup:ListProtectedResourcesByBackupVault",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListRecoveryPointsByResource",
        "backup:ListTags",
        "backup:StartRestoreJob"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "IamPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters",
        "redshift:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:TerminateInstances",
        "elasticfilesystem:DeleteFilesystem",
        "elasticfilesystem:DeleteMountTarget",
        "rds:DeleteDBCluster",
        "rds:DeleteDBInstance",
        "rds:DeleteTenantDatabase",
```

```
        "fsx:DeleteFileSystem",
        "fsx:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/awsbackup-restore-test" : "false"
        }
      }
    },
    {
      "Sid" : "DdbDeleteActions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/awsbackup-restore-test-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftDeleteActions",
      "Effect" : "Allow",
      "Action" : "redshift:DeleteCluster",
      "Resource" : "arn:aws:redshift:*:*:cluster:awsbackup-restore-test-*"
    },
    {
      "Sid" : "S3DeleteActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::awsbackup-restore-test-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "TimestreamDeleteActions",
      "Effect" : "Allow",
      "Action" : "timestream:DeleteTable",
      "Resource" : "arn:aws:timestream:*:*:database/*/table/awsbackup-restore-test-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSServiceRolePolicyForWorkspacesInstances

Deskripsi: Kebijakan terkelola ini menyediakan akses administratif WorkSpaces ke Amazon untuk mengelola instans EC2 di Akun AWS

`AWSServiceRolePolicyForWorkspacesInstances`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 11 Juni 2025, 20:37 UTC
- Waktu teredit: 27 Agustus 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForWorkspacesInstances`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateCapacityReservation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateCapacityReservation",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ManagedBy" : "workspaces-instances"
        }
      }
    },
    {
      "Sid" : "ManageTaggedCapacityReservations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyCapacityReservation",
        "ec2:CancelCapacityReservation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/ManagedBy" : "workspaces-instances"
        }
      }
    },
    {
      "Sid" : "TagRemediation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:capacity-reservation/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ManagedBy" : "workspaces-instances"
        }
      }
    },
    {
      "Sid" : "ManagedInstanceOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:TerminateInstances",
        "ec2:DeleteVolume",
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ManagedResourceOperator" : "workspaces-instances.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSShieldDRTAccessPolicy

Deskripsi: Memberikan Tim Resp AWS ons DDoS akses terbatas ke Anda Akun AWS untuk membantu mitigasi serangan DDoS selama peristiwa tingkat keparahan tinggi.

`AWSShieldDRTAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSShieldDRTAccessPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Juni 2018, 22:29 UTC
- Waktu teredit: 15 Desember 2020, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SRTAccessProtectedResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:List*",
        "route53:List*",
        "elasticloadbalancing:Describe*",
        "cloudwatch:Describe*",
```

```
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudfront:GetDistribution*",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:DescribeAccelerator",
        "ec2:DescribeRegions",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SRTManageProtections",
      "Effect" : "Allow",
      "Action" : [
        "shield:*",
        "waf:*",
        "wafv2:*",
        "waf-regional:*",
        "elasticloadbalancing:SetWebACL",
        "cloudfront:UpdateDistribution",
        "apigateway:SetWebACL"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSShieldServiceRolePolicy

Deskripsi: Men AWS gizinkan Shield mengakses AWS sumber daya atas nama Anda untuk memberikan perlindungan DDoS.

`AWSShieldServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 17 November 2021, 19:17 UTC
- Waktu teredit: 17 November 2021, 19.17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSShield",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:UpdateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSocialMessagingServiceRolePolicy

Deskripsi: Menyediakan akses untuk mempublikasikan metrik dan memberikan wawasan untuk pengiriman pesan sosial Anda.

`AWSSocialMessagingServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 10 Oktober 2024, 19:28 UTC
- Waktu teredit: 10 Oktober 2024, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSocialMessagingServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudwatchMetricPublishing",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/SocialMessaging"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSSMForSAPServiceLinkedRolePolicy

Deskripsi: Men AWS yediakan Manajer Sistem untuk SAP dengan izin yang diperlukan untuk mengelola dan mengintegrasikan perangkat lunak SAP dengan AWS.

`AWSSSMForSAPServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 16 November 2022, 01:18 UTC
- Waktu teredit: 12 Februari 2026, 18:03 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v21 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstanceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcs",
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstanceStatus",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstanceStatus",
      "Resource" : "*"
    },
    {
      "Sid" : "TargetRuleActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:*:events:*:*:rule/SSMSAPManagedRule*",
        "arn:*:events:*:*:event-bus/default"
      ]
    },
    {
      "Sid" : "DocumentActions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:*:ssm:*:*:document/AWSSystemsManagerSAP-*",
        "arn:*:ssm:*:*:document/AWSSSMSAP*",
        "arn:*:ssm:*:*:document/AWSSAP*"
      ]
    },
    {
      "Sid" : "CustomerSendCommand",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "ssm:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "InstanceTagActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
```

```
        "Null" : {
          "aws:RequestTag/awsApplication" : "false"
        },
        "StringEqualsIgnoreCase" : {
          "ec2:ResourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "DescribeTag",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeTags",
      "Resource" : "*"
    },
    {
      "Sid" : "GetApplication",
      "Effect" : "Allow",
      "Action" : "servicecatalog:GetApplication",
      "Resource" : "arn:*:servicecatalog:*:*:*"
    },
    {
      "Sid" : "UpdateOrDeleteApplication",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:DeleteApplication",
        "servicecatalog:UpdateApplication"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateApplication",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TagResource",
        "servicecatalog:CreateApplication"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/servicecatalog-
appregistry.amazonaws.com/AWSServiceRoleForAWSServiceCatalogAppRegistry",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PutMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Usage",
            "AWS/SSMForSAP"
          ]
        }
      }
    },
    {
      "Sid" : "CreateAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:CreateAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "GetAttributeGroup",
      "Effect" : "Allow",
```

```
      "Action" : "servicecatalog:GetAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*"
    },
    {
      "Sid" : "DeleteAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:DeleteAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "AttributeGroupActions",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "ListAssociatedAttributeGroups",
      "Effect" : "Allow",
      "Action" : "servicecatalog:ListAssociatedAttributeGroups",
      "Resource" : "arn:*:servicecatalog:*:*:*"
    },
    {
      "Sid" : "CreateGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SSMForSAPCreated"
          ]
        }
      }
    },
    {
      "Sid" : "GetGroup",
      "Effect" : "Allow",
      "Action" : "resource-groups:GetGroup",
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*"
    },
    {
      "Sid" : "DeleteGroup",
      "Effect" : "Allow",
      "Action" : "resource-groups:DeleteGroup",
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateAppTagResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Sid" : "TagAppTagResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:Tag"
```

```
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Sid" : "GetAppTagResourceGroupConfig",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupConfiguration"
      ],
      "Resource" : [
        "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*"
      ]
    },
    {
      "Sid" : "StartStopInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "ec2:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "SsmSapResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:Tag",
        "resource-groups:CreateGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SSMForSAPCreated" : "True"
        },
```

```
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SSMForSAPCreated"
          ]
        }
      }
    },
    {
      "Sid" : "ManageSsmSapTagsOnEc2Instances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPManaged" : "True"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "SystemsManagerForSAP-*"
          ]
        }
      }
    },
    {
      "Sid" : "ManageSsmSapTagsOnEbsVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "SystemsManagerForSAP-*"
          ]
        }
      }
    },
    {
      "Sid" : "ManageAppTagsOnEbsVolumes",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/awsApplication" : "arn:aws:resource-groups:*:*:group/*/*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "awsApplication"
          ]
        }
      }
    },
    {
      "Sid" : "ManageCostAllocationTags",
      "Effect" : "Allow",
      "Action" : [
        "ce:ListCostAllocationTags",
        "ce:UpdateCostAllocationTagsStatus",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:StartCostAllocationTagBackfill"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSSMOpsInsightsServiceRolePolicy

Deskripsi: Kebijakan untuk Peran Terkait Layanan AWSServiceRoleForAmazonSSM _ OpsInsights

`AWSSSMOpsInsightsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 16 Juni 2021, 20:12 UTC
- Waktu teredit: 16 Juni 2021, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMOpsInsightsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessOpsItem",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:UpdateOpsItem",
        "ssm:GetOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SsmOperationalInsight" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSSODirectoryAdministrator

Deskripsi: Akses administrator untuk Direktori SSO

`AWSSSODirectoryAdministrator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSSODirectoryAdministrator` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 31 Oktober 2018, 23:54 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSSODirectoryReadOnly

Deskripsi: ReadOnly akses untuk Direktori SSO

`AWSSSODirectoryReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSSODirectoryReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 31 Oktober 2018, 23:49 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:Search*",
```

```
        "sso-directory:Describe*",
        "sso-directory:List*",
        "sso-directory:Get*",
        "identitystore:Describe*",
        "identitystore:List*",
        "identitystore-auth:ListSessions",
        "identitystore-auth:BatchGetSession"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSSOMasterAccountAdministrator

Deskripsi: Menyediakan akses dalam AWS SSO untuk mengelola AWS akun master dan anggota Organisasi serta aplikasi cloud

`AWSSSOMasterAccountAdministrator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSSOMasterAccountAdministrator` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2018, 20:36 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator`

Versi kebijakan

Versi kebijakan: v13 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMasterAccountAdministrator",
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeTrusts",
        "ds:UnauthorizeApplication",
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:DescribeOrganization",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy",
        "signin:CreateTrustedIdentityPropagationApplicationForConsole",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSSOManageDelegatedAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
```

```
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowDeleteSyncProfile",
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:DeleteSyncProfile"
      ],
      "Resource" : [
        "arn:aws:identity-sync:*:*:profile/*"
      ]
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIAMIdentityCenterService",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSSOMemberAccountAdministrator

Deskripsi: Menyediakan akses dalam AWS SSO untuk mengelola akun anggota AWS Organisasi dan aplikasi cloud

`AWSSSOMemberAccountAdministrator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSSOMemberAccountAdministrator` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2018, 20:45 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMemberAccountAdministrator`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
```

```
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy",
        "signin:CreateTrustedIdentityPropagationApplicationForConsole",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSSOManageDelegatedAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIAMIdentityCenterService",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSSOReadOnly

Deskripsi: Menyediakan akses baca saja ke konfigurasi AWS SSO.

`AWSSSOReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSSOReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2018, 20:24 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOReadOnly`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "sso:Search*",
```

```
        "sso-directory:DescribeDirectory",
        "access-analyzer:ValidatePolicy",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIAMIdentityCenterService",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSSOServiceRolePolicy

Deskripsi: Memberikan izin AWS SSO untuk mengelola AWS sumber daya, termasuk peran IAM, kebijakan, dan IdP SAML atas nama Anda.

`AWSSSOServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 05 Desember 2017, 18:36 UTC
- Waktu teredit: 11 Februari 2025, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSOServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v18 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMRoleProvisioningActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:UpdateRole",
```

```
        "iam:UpdateRoleDescription",
        "iam:UpdateAssumeRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:DeleteRolePermissionsBoundary"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalOrgMasterAccountId" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMRoleReadActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMRoleCleanupActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
      ]
    },
    {
      "Sid" : "IAMSLRCleanupActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
```

```
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:DeleteRole",
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO"
      ]
    },
    {
      "Sid" : "IAMSAMLProviderCreationAction",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateSAMLProvider"
      ],
      "Resource" : [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalOrgMasterAccountId" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMSAMLProviderUpdateAction",
      "Effect" : "Allow",
      "Action" : [
        "iam:UpdateSAMLProvider"
      ],
      "Resource" : [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ]
    },
    {
      "Sid" : "IAMSAMLProviderCleanupActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSAMLProvider",
        "iam:GetSAMLProvider"
      ],
      "Resource" : [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowUnauthAppForDirectory",
      "Effect" : "Allow",
      "Action" : [
        "ds:UnauthorizeApplication"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeForDirectory",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:DescribeTrusts"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeAndListOperationsOnIdentitySource",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "identitystore:DescribeGroup",
        "identitystore:ListGroups",
        "identitystore:ListUsers"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "AllowDeleteSyncProfile",
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:DeleteSyncProfile"
      ],
      "Resource" : [
        "arn:aws:identity-sync:*:*:profile/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSStepFunctionsConsoleFullAccess

Deskripsi: Kebijakan akses untuk menyediakan akses user/role /etc ke AWS StepFunctions konsol. Untuk pengalaman konsol penuh, selain kebijakan ini, pengguna mungkin memerlukan PassRole izin iam: pada peran IAM lain yang dapat diasumsikan oleh layanan.

`AWSStepFunctionsConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSStepFunctionsConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Januari 2017, 21:54 UTC
- Waktu teredit: 12 Januari 2017, 00:19 UTC

- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "states:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/StatesExecutionRole*"
    },
    {
      "Effect" : "Allow",
      "Action" : "lambda:ListFunctions",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSStepFunctionsFullAccess

Deskripsi: Kebijakan akses untuk menyediakan akses user/role /etc ke AWS StepFunctions API. Untuk akses penuh, selain kebijakan ini, pengguna HARUS memiliki PassRole izin iam: pada setidaknya satu peran IAM yang dapat diasumsikan oleh layanan.

`AWSStepFunctionsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSStepFunctionsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Januari 2017, 21:51 UTC
- Waktu teredit: 11 Januari 2017, 21:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : "states:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSStepFunctionsReadOnlyAccess

Deskripsi: Kebijakan akses untuk menyediakan akses baca saja user/role /etc ke AWS StepFunctions layanan.

`AWSStepFunctionsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSStepFunctionsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Januari 2017, 21:46 UTC
- Waktu teredit: 26 April 2024, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "states:ListStateMachines",
        "states:ListActivities",
        "states:DescribeStateMachine",
        "states:DescribeStateMachineForExecution",
        "states:ListExecutions",
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:DescribeActivity",
        "states:ListTagsForResource",
        "states:DescribeMapRun",
        "states:ListMapRuns",
        "states:DescribeStateMachineAlias",
        "states:ListStateMachineAliases",
        "states:ListStateMachineVersions",
        "states:ValidateStateMachineDefinition"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSStorageGatewayFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Storage Gateway melalui Konsol Manajemen AWS.

`AWSStorageGatewayFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSStorageGatewayFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 06 September 2022, 20.26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "fetchStorageGatewayParams",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameters",
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/storagegateway/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSStorageGatewayReadOnlyAccess

Deskripsi: Menyediakan akses ke AWS Storage Gateway melalui Konsol Manajemen AWS.

`AWSStorageGatewayReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSStorageGatewayReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 06 September 2022, 20.24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:List*",
        "storagegateway:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "fetchStorageGatewayParams",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameters",
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/storagegateway/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSStorageGatewayServiceRolePolicy

Deskripsi: Service-linked peran yang digunakan oleh AWS Storage Gateway untuk mengaktifkan integrasi AWS layanan lain dengan Storage Gateway.

`AWSStorageGatewayServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 17 Februari 2021, 19:03 UTC
- Waktu teredit: 17 Februari 2021, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "fsx:ListTagsForResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSupplyChainFederationAdminAccess

Deskripsi: AWSSupplyChainFederationAdminAccess menyediakan AWS akses pengguna federasi Supply Chain ke aplikasi Sup AWS ply Chain, termasuk izin yang diperlukan untuk melakukan tindakan dalam aplikasi Sup AWS ply Chain. Kebijakan ini memberikan izin administratif atas pengguna dan grup Pusat Identitas IAM dan dilampirkan ke peran yang dibuat oleh Sup AWS ply Chain atas nama Anda. Anda tidak boleh melampirkan AWSSupplyChainFederationAdminAccess kebijakan ke entitas IAM lainnya.

`AWSSupplyChainFederationAdminAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSupplyChainFederationAdminAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Maret 2023, 18:54 UTC
- Waktu teredit: 14 Agustus 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSupplyChain",
      "Effect" : "Allow",
      "Action" : [
        "scn:*"
      ],
      "Resource" : [
        "arn:aws:scn:*:*:instance/*"
      ]
    },
    {
      "Sid" : "ChimeAppInstance",
      "Effect" : "Allow",
      "Action" : [
        "chime:BatchCreateChannelMembership",
        "chime:CreateAppInstanceUser",
        "chime:CreateChannel",
        "chime:CreateChannelMembership",
        "chime:CreateChannelModerator",
        "chime:Connect",
        "chime:DeleteChannelMembership",
        "chime:DeleteChannelModerator",
        "chime:DescribeChannelMembershipForAppInstanceUser",
        "chime:GetChannelMembershipPreferences",
        "chime:ListChannelMemberships",
        "chime:ListChannelMembershipsForAppInstanceUser",
        "chime:ListChannelMessages",
        "chime:ListChannelModerators",
        "chime:TagResource",
        "chime:PutChannelMembershipPreferences",
```

```
        "chime:SendChannelMessage",
        "chime:UpdateChannelReadMarker",
        "chime:UpdateAppInstanceUser"
      ],
      "Resource" : [
        "arn:aws:chime:*:*:app-instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/SCNInstanceId" : "*"
        }
      }
    },
    {
      "Sid" : "ChimeChannel",
      "Effect" : "Allow",
      "Action" : [
        "chime:DescribeChannel"
      ],
      "Resource" : [
        "arn:aws:chime:*:*:app-instance/*"
      ]
    },
    {
      "Sid" : "ChimeMessaging",
      "Effect" : "Allow",
      "Action" : [
        "chime:GetMessagingSessionEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso:ListDirectoryAssociations",
        "sso:AssociateProfile",
        "sso:DisassociateProfile",
        "sso:ListProfiles",
        "sso:GetProfile",
        "sso:ListProfileAssociations",
        "sso:ListApplicationAssignments",
        "sso:DescribeApplication",
```

```
        "sso:DescribeInstance",
        "sso:GetApplicationAssignmentConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BuilderIDCollaboration",
      "Effect" : "Allow",
      "Action" : [
        "builderid:CreateInvitation",
        "builderid:ListInvitations",
        "builderid:DeleteInvitation",
        "builderid:DisassociateCollaborator"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IdentityStoreCollaboration",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:ReserveUser",
        "identitystore:DeleteUser"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AppflowConnectorProfile",
      "Effect" : "Allow",
      "Action" : [
        "appflow:CreateConnectorProfile",
        "appflow:UseConnectorProfile",
        "appflow:DeleteConnectorProfile",
        "appflow:UpdateConnectorProfile"
      ],
      "Resource" : [
        "arn:aws:appflow:*:*:connectorprofile/scn-*"
      ]
    },
    {
```

```
      "Sid" : "AppflowFlow",
      "Effect" : "Allow",
      "Action" : [
        "appflow:CreateFlow",
        "appflow:DeleteFlow",
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:ListFlows",
        "appflow:StartFlow",
        "appflow:StopFlow",
        "appflow:UpdateFlow",
        "appflow:TagResource",
        "appflow:UntagResource"
      ],
      "Resource" : [
        "arn:aws:appflow:*:*:flow/scn-*"
      ]
    },
    {
      "Sid" : "S3ListAllBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ListSupplyChainBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-supply-chain-data-*"
      ]
    },
    {
      "Sid" : "S3ReadWriteObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::aws-supply-chain-data-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerCreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "appflow!*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecretsManagerPutResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        },
        "StringEqualsIgnoreCase" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "appflow"
        }
      }
    },
```

```
    {
      "Sid" : "KMSListKeys",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "KMSListGrants",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListGrants"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceTag/aws-supply-chain-access" : "true"
        }
      }
    },
    {
      "Sid" : "KMSCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringEquals" : {
          "aws:ResourceTag/aws-supply-chain-access" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSupportAccess

Deskripsi: Memungkinkan pengguna mengakses AWS Dukungan Pusat.

`AWSSupportAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSupportAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:*",
        "support-console:*"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSupportAppFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Dukungan Aplikasi dan layanan lain yang diperlukan, seperti AWS Dukungan dan Kuota Layanan. Kebijakan ini mencakup izin untuk menggunakan layanan pendukung sehingga pengguna dapat menghubungi AWS Dukungan untuk kasus dukungan, mengubah kuota layanan, dan membuat peran terkait layanan yang relevan.

`AWSSupportAppFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSupportAppFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 Agustus 2022, 16:53 UTC
- Waktu teredit: 22 Agustus 2022, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:RequestServiceQuotaIncrease",
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:DescribeSeverityLevels",
        "support:InitiateChatForCase",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicequotas.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSupportAppReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke Aplikasi. AWS Dukungan

`AWSSupportAppReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSupportAppReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 Agustus 2022, 17:01 UTC
- Waktu teredit: 22 Agustus 2022, 17.01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeCases",
```

```
        "support:DescribeCommunications"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSupportPlansFullAccess

Deskripsi: Menyediakan akses penuh ke paket dukungan.

`AWSSupportPlansFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSupportPlansFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 September 2022, 18:19 UTC
- Waktu teredit: 24 Agustus 2026, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:ListSupportPlanModifiers",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:CreateSupportPlanSchedule",
        "supportplans:AcceptSupportAgreement",
        "supportplans:CancelSupportAgreement",
        "supportplans:CreateSupportAgreement",
        "supportplans:GetSupportAgreement",
        "supportplans:ListSupportAgreements",
        "supportplans:ListSupportAgreementRevisions",
        "supportplans:RejectSupportAgreement",
        "supportplans:UpdateSupportAgreement"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/supportplans.amazonaws.com/
AWSServiceRoleForSupportPlans",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "supportplans.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/supportplans.amazonaws.com/
AWSServiceRoleForSupportPlans"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSupportPlansReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke rencana dukungan.

`AWSSupportPlansReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSupportPlansReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 September 2022, 18:08 UTC
- Waktu teredit: 24 Agustus 2026, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:ListSupportPlanModifiers",
        "supportplans:GetSupportAgreement",
        "supportplans:ListSupportAgreements",
        "supportplans:ListSupportAgreementRevisions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSupportPlansServiceRolePolicy

Deskripsi: Men AWS Dukungan gizinkan Paket membaca dan memperbarui AWS sumber daya yang digunakan untuk mengelola Rencana Dukungan akun Anda atas nama Anda.

`AWSSupportPlansServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 31 Juli 2026, 17:12 UTC

- Waktu teredit: 31 Juli 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSupportPlansServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:AcceptSupportAgreement",
        "supportplans:CancelSupportAgreement",
        "supportplans:CreateSupportAgreement",
        "supportplans:GetSupportAgreement",
        "supportplans:ListSupportAgreements",
        "supportplans:ListSupportAgreementRevisions",
        "supportplans:RejectSupportAgreement",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:UpdateSupportAgreement",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSupportServiceRolePolicy

Deskripsi: Memungkinkan AWS Dukungan untuk mengakses AWS sumber daya untuk menyediakan layanan penagihan, administrasi, dan dukungan.

`AWSSupportServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 19 April 2018, 18:04 UTC
- Waktu teredit: 19 Agustus 2026, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v59 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSupportAPIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/account",
```

```
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*:*:/domainnameaccessassociations",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/domainnames/*/apimappings/*",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models/*/default_template",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration/responses/
*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/responses/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*/sdks/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
```

```
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "AWSSupportDeleteRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/support.amazonaws.com/
AWSServiceRoleForSupport"
      ]
    },
    {
      "Sid" : "AWSSupportActionsGroup1",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:getAccessPreview",
        "access-analyzer:getAnalyzedResource",
        "access-analyzer:getAnalyzer",
        "access-analyzer:getArchiveRule",
        "access-analyzer:getFinding",
        "access-analyzer:getGeneratedPolicy",
        "access-analyzer:listAccessPreviewFindings",
        "access-analyzer:listAccessPreviews",
        "access-analyzer:listAnalyzedResources",
        "access-analyzer:listAnalyzers",
        "access-analyzer:listArchiveRules",
        "access-analyzer:listFindings",
        "access-analyzer:listPolicyGenerations",
        "account:getRegionOptStatus",
        "account:listRegions",
        "acm-pca:describeCertificateAuthority",
        "acm-pca:describeCertificateAuthorityAuditReport",
        "acm-pca:getCertificate",
        "acm-pca:getCertificateAuthorityCertificate",
        "acm-pca:getCertificateAuthorityCsr",
        "acm-pca:listCertificateAuthorities",
```

```
        "acm-pca:listTags",
        "acm:describeAcmeAccount",
        "acm:describeAcmeDomainValidation",
        "acm:describeAcmeEndpoint",
        "acm:describeAcmeExternalAccountBinding",
        "acm:describeCertificate",
        "acm:getAccountConfiguration",
        "acm:getCertificate",
        "acm:listAcmeAccounts",
        "acm:listAcmeDomainValidations",
        "acm:listAcmeEndpoints",
        "acm:listAcmeExternalAccountBindings",
        "acm:listCertificates",
        "acm:listTagsForCertificate",
        "acm:searchCertificates",
        "aidevops:describePrivateConnection",
        "aidevops:getAccountUsage",
        "aidevops:getAgentSpace",
        "aidevops:getAssociation",
        "aidevops:getBacklogTask",
        "aidevops:getOperatorApp",
        "aidevops:getRecommendation",
        "aidevops:getService",
        "aidevops:listAgentSpaces",
        "aidevops:listAssociations",
        "aidevops:listBacklogTasks",
        "aidevops:listChats",
        "aidevops:listExecutions",
        "aidevops:listGoals",
        "aidevops:listPrivateConnections",
        "aidevops:listRecommendations",
        "aidevops:listServices",
        "aidevops:listWebHooks",
        "aiops:getInvestigationGroup",
        "aiops:getInvestigationGroupPolicy",
        "aiops:listInvestigationGroups",
        "airflow-serverless:getTaskInstance",
        "airflow-serverless:getWorkflow",
        "airflow-serverless:getWorkflowRun",
        "airflow-serverless:listTaskInstances",
        "airflow-serverless:listWorkflowRuns",
        "airflow-serverless:listWorkflows",
        "airflow-serverless:listWorkflowVersions",
        "airflow:getEnvironment",
```

```
        "airflow:listEnvironments",
        "airflow:listTagsForResource",
        "amplify:getApp",
        "amplify:getBackendEnvironment",
        "amplify:getBranch",
        "amplify:getDomainAssociation",
        "amplify:getJob",
        "amplify:getWebhook",
        "amplify:listApps",
        "amplify:listBackendEnvironments",
        "amplify:listBranches",
        "amplify:listDomainAssociations",
        "amplify:listJobs",
        "amplify:listResourcesForWebACL",
        "amplify:listWebhooks",
        "amplifyuibuilder:exportComponents",
        "amplifyuibuilder:exportThemes",
        "apigateway:getPortal",
        "apigateway:getPortalProduct",
        "apigateway:getPortalProductSharingPolicy",
        "apigateway:getProductPage",
        "apigateway:getProductRestEndpointPage",
        "apigateway:getRoutingRule",
        "apigateway:listPortalProducts",
        "apigateway:listPortals",
        "apigateway:listProductPages",
        "apigateway:listProductRestEndpointPages",
        "apigateway:listRoutingRules",
        "aoss:batchGetCollection",
        "aoss:batchGetCollectionGroup",
        "aoss:batchGetEffectiveLifecyclePolicy",
        "aoss:batchGetLifecyclePolicy",
        "aoss:batchGetVpcEndpoint",
        "aoss:getAccessPolicy",
        "aoss:getAccountSettings",
        "aoss:getIndex",
        "aoss:getPoliciesStats",
        "aoss:getSecurityConfig",
        "aoss:getSecurityPolicy",
        "aoss:listAccessPolicies",
        "aoss:listCollectionGroups",
        "aoss:listCollections",
        "aoss:listLifecyclePolicies",
        "aoss:listSecurityConfigs",
```

```
        "aoss:listSecurityPolicies",
        "aoss:listTagsForResource",
        "aoss:listVpcEndpoints",
        "appconfig:getAccountSettings",
        "appconfig:getApplication",
        "appconfig:getConfigurationProfile",
        "appconfig:getDeployment",
        "appconfig:getDeploymentStrategy",
        "appconfig:getEnvironment",
        "appconfig:getExtension",
        "appconfig:getExtensionAssociation",
        "appconfig:getHostedConfigurationVersion",
        "appconfig:listApplications",
        "appconfig:listConfigurationProfiles",
        "appconfig:listDeployments",
        "appconfig:listDeploymentStrategies",
        "appconfig:listEnvironments",
        "appconfig:listExtensionAssociations",
        "appconfig:listExtensions",
        "appconfig:listHostedConfigurationVersions",
        "appflow:describeConnectorEntity",
        "appflow:describeConnectorProfiles",
        "appflow:describeConnectors",
        "appflow:describeFlow",
        "appflow:describeFlowExecutionRecords",
        "appflow:listConnectorEntities",
        "appflow:listFlows",
        "application-autoscaling:describeScalableTargets",
        "application-autoscaling:describeScalingActivities",
        "application-autoscaling:describeScalingPolicies",
        "application-autoscaling:describeScheduledActions",
        "application-signals:getService",
        "application-signals:getServiceLevelObjective",
        "application-signals:listServiceDependencies",
        "application-signals:listServiceDependents",
        "application-signals:listServiceLevelObjectives",
        "application-signals:listServiceOperations",
        "application-signals:listServices",
        "applicationinsights:describeApplication",
        "applicationinsights:describeComponent",
        "applicationinsights:describeComponentConfiguration",
        "applicationinsights:describeComponentConfigurationRecommendation",
        "applicationinsights:describeLogPattern",
        "applicationinsights:describeObservation",
```

```
        "applicationinsights:describeProblem",
        "applicationinsights:describeProblemObservations",
        "applicationinsights:listApplications",
        "applicationinsights:listComponents",
        "applicationinsights:listConfigurationHistory",
        "applicationinsights:listLogPatterns",
        "applicationinsights:listLogPatternSets",
        "applicationinsights:listProblems",
        "appmesh:describeGatewayRoute",
        "appmesh:describeMesh",
        "appmesh:describeRoute",
        "appmesh:describeVirtualGateway",
        "appmesh:describeVirtualNode",
        "appmesh:describeVirtualRouter",
        "appmesh:describeVirtualService",
        "appmesh:listGatewayRoutes",
        "appmesh:listMeshes",
        "appmesh:listRoutes",
        "appmesh:listTagsForResource",
        "appmesh:listVirtualGateways",
        "appmesh:listVirtualNodes",
        "appmesh:listVirtualRouters",
        "appmesh:listVirtualServices",
        "apprunner:describeAutoScalingConfiguration",
        "apprunner:describeCustomDomains",
        "apprunner:describeObservabilityConfiguration",
        "apprunner:describeOperation",
        "apprunner:describeService",
        "apprunner:describeVpcConnector",
        "apprunner:describeVpcIngressConnection",
        "apprunner:listAutoScalingConfigurations",
        "apprunner:listConnections",
        "apprunner:listObservabilityConfigurations",
        "apprunner:listOperations",
        "apprunner:listAssociatedServicesForWebAcl",
        "apprunner:listServices",
        "apprunner:listTagsForResource",
        "apprunner:listVpcConnectors",
        "apprunner:listVpcIngressConnections",
        "appstream:describeAppBlockBuilderAppBlockAssociations",
        "appstream:describeAppBlockBuilders",
        "appstream:describeAppBlocks",
        "appstream:describeApplicationFleetAssociations",
        "appstream:describeApplications",
```

```
        "appstream:describeDirectoryConfigs",
        "appstream:describeEntitlements",
        "appstream:describeFleets",
        "appstream:describeImageBuilders",
        "appstream:describeImagePermissions",
        "appstream:describeImages",
        "appstream:describeSessions",
        "appstream:describeStacks",
        "appstream:describeUsageReportSubscriptions",
        "appstream:describeUsers",
        "appstream:describeUserStackAssociations",
        "appstream:listAssociatedFleets",
        "appstream:listAssociatedStacks",
        "appstream:listEntitledApplications",
        "appstream:listTagsForResource",
        "appsync:evaluateCode",
        "appsync:evaluateMappingTemplate",
        "appsync:getApi",
        "appsync:getApiAssociation",
        "appsync:getApiCache",
        "appsync:getChannelNamespace",
        "appsync:getDataSource",
        "appsync:getDataSourceIntrospection",
        "appsync:getDomainName",
        "appsync:getFunction",
        "appsync:getGraphqlApi",
        "appsync:getGraphqlApiEnvironmentVariables",
        "appsync:getIntrospectionSchema",
        "appsync:getResolver",
        "appsync:getSchemaCreationStatus",
        "appsync:getSourceApiAssociation",
        "appsync:getType",
        "appsync:listApis",
        "appsync:listChannelNamespaces",
        "appsync:listDataSources",
        "appsync:listDomainNames",
        "appsync:listFunctions",
        "appsync:listGraphqlApis",
        "appsync:listResolvers",
        "appsync:listResolversByFunction",
        "appsync:listSourceApiAssociations",
        "appsync:listTypes",
        "appsync:listTypesByAssociation",
        "aps:describeAlertManagerDefinition",
```

```
        "aps:describeRuleGroupsNamespace",
        "aps:describeScraper",
        "aps:describeWorkspace",
        "aps:listRuleGroupsNamespaces",
        "aps:listScrapers",
        "aps:listWorkspaces",
        "arc-zonal-shift:getAutoshiftObserverNotificationStatus",
        "arc-zonal-shift:getManagedResource",
        "arc-zonal-shift:listAutoshifts",
        "arc-zonal-shift:listManagedResources",
        "arc-zonal-shift:listZonalShifts",
        "athena:batchGetNamedQuery",
        "athena:batchGetQueryExecution",
        "athena:getCalculationExecution",
        "athena:getCalculationExecutionStatus",
        "athena:getCapacityAssignmentConfiguration",
        "athena:getCapacityReservation",
        "athena:getDataCatalog",
        "athena:getNamedQuery",
        "athena:getNotebookMetadata",
        "athena:getQueryExecution",
        "athena:getQueryRuntimeStatistics",
        "athena:getSession",
        "athena:getSessionStatus",
        "athena:getWorkGroup",
        "athena:listApplicationDPUSizes",
        "athena:listCalculationExecutions",
        "athena:listCapacityReservations",
        "athena:listDataCatalogs",
        "athena:listEngineVersions",
        "athena:listExecutors",
        "athena:listNamedQueries",
        "athena:listNotebookMetadata",
        "athena:listNotebookSessions",
        "athena:listQueryExecutions",
        "athena:listSessions",
        "athena:listTagsForResource",
        "athena:listWorkGroups",
        "auditmanager:getAccountStatus",
        "auditmanager:getDelegations",
        "auditmanager:listAssessmentFrameworks",
        "auditmanager:listAssessmentReports",
        "auditmanager:listAssessments",
        "auditmanager:listControls",
```

```
        "auditmanager:listKeywordsForDataSource",
        "auditmanager:listNotifications",
        "autoscaling-plans:describeScalingPlanResources",
        "autoscaling-plans:describeScalingPlans",
        "autoscaling-plans:getScalingPlanResourceForecastData",
        "autoscaling:describeAccountLimits",
        "autoscaling:describeAdjustmentTypes",
        "autoscaling:describeAutoScalingGroups",
        "autoscaling:describeAutoScalingInstances",
        "autoscaling:describeAutoScalingNotificationTypes",
        "autoscaling:describeInstanceRefreshes",
        "autoscaling:describeLaunchConfigurations",
        "autoscaling:describeLifecycleHooks",
        "autoscaling:describeLifecycleHookTypes",
        "autoscaling:describeLoadBalancers",
        "autoscaling:describeLoadBalancerTargetGroups",
        "autoscaling:describeMetricCollectionTypes",
        "autoscaling:describeNotificationConfigurations",
        "autoscaling:describePolicies",
        "autoscaling:describeScalingActivities",
        "autoscaling:describeScalingProcessTypes",
        "autoscaling:describeScheduledActions",
        "autoscaling:describeTags",
        "autoscaling:describeTerminationPolicyTypes",
        "autoscaling:describeTrafficSources",
        "autoscaling:describeWarmPool",
        "aws-marketplace:describeAgreement",
        "aws-marketplace:describeEntity",
        "aws-marketplace:listEntities",
        "aws-marketplace:searchAgreements",
        "backup-gateway:getBandwidthRateLimitSchedule",
        "backup-gateway:getGateway",
        "backup-gateway:getHypervisor",
        "backup-gateway:getHypervisorPropertyMappings",
        "backup-gateway:getVirtualMachine",
        "backup-gateway:listGateways",
        "backup-gateway:listHypervisors",
        "backup-gateway:listVirtualMachines",
        "backup-gateway:listTagsForResource",
        "backup-search:getSearchJob",
        "backup-search:getSearchResultExportJob",
        "backup-search:listSearchJobBackups",
        "backup-search:listSearchJobs",
        "backup-search:listSearchResultExportJobs",
```

```
        "backup-search:listTagsForResource",
        "backup:describeBackupAccessPoint",
        "backup:describeScanJob",
        "backup:describeBackupJob",
        "backup:describeBackupVault",
        "backup:describeCopyJob",
        "backup:describeFramework",
        "backup:describeGlobalSettings",
        "backup:describeProtectedResource",
        "backup:describeRecoveryPoint",
        "backup:describeRegionSettings",
        "backup:describeReportJob",
        "backup:describeReportPlan",
        "backup:describeRestoreJob",
        "backup:getBackupPlan",
        "backup:getBackupPlanFromJSON",
        "backup:getBackupPlanFromTemplate",
        "backup:getBackupSelection",
        "backup:getBackupVaultAccessPolicy",
        "backup:getBackupVaultNotifications",
        "backup:getLegalHold",
        "backup:getRecoveryPointRestoreMetadata",
        "backup:getRecoveryPointIndexDetails",
        "backup:getRestoreJobMetadata",
        "backup:getRestoreTestingInferredMetadata",
        "backup:getRestoreTestingPlan",
        "backup:getRestoreTestingSelection",
        "backup:getSupportedResourceTypes",
        "backup:getTieringConfiguration",
        "backup:listBackupJobs",
        "backup:listBackupJobSummaries",
        "backup:listBackupPlans",
        "backup:listBackupPlanTemplates",
        "backup:listBackupPlanVersions",
        "backup:listBackupSelections",
        "backup:listBackupVaults",
        "backup:listCopyJobs",
        "backup:listCopyJobSummaries",
        "backup:listFrameworks",
        "backup:listIndexedRecoveryPoints",
        "backup:listLegalHolds",
        "backup:listProtectedResources",
        "backup:listProtectedResourcesByBackupVault",
        "backup:listRecoveryPointsByBackupVault",
```

```
        "backup:listRecoveryPointsByLegalHold",
        "backup:listRecoveryPointsByResource",
        "backup:listReportJobs",
        "backup:listReportPlans",
        "backup:listRestoreAccessBackupVaults",
        "backup:listRestoreJobs",
        "backup:listRestoreJobsByProtectedResource",
        "backup:listRestoreJobSummaries",
        "backup:listRestoreTestingPlans",
        "backup:listRestoreTestingSelections",
        "backup:listScanJobSummaries",
        "backup:listScanJobs",
        "backup:listTags",
        "backup:listTieringConfigurations",
        "batch:describeComputeEnvironments",
        "batch:describeConsumableResource",
        "batch:describeJobDefinitions",
        "batch:describeJobQueues",
        "batch:describeJobs",
        "batch:describeSchedulingPolicies",
        "batch:describeServiceEnvironments",
        "batch:describeServiceJob",
        "batch:getJobQueueSnapshot",
        "batch:listConsumableResources",
        "batch:listJobs",
        "batch:listJobsByConsumableResource",
        "batch:listSchedulingPolicies",
        "batch:listServiceJobs",
        "batch:listTagsForResource",
        "bedrock:exportAutomatedReasoningPolicyVersion",
        "bedrock:getAgent",
        "bedrock:getAgentActionGroup",
        "bedrock:getAgentAlias",
        "bedrock:getAgentKnowledgeBase",
        "bedrock:getAgentMemory",
        "bedrock:getAgentVersion",
        "bedrock:getAsyncInvoke",
        "bedrock:getAutomatedReasoningPolicy",
        "bedrock:getAutomatedReasoningPolicyAnnotations",
        "bedrock:getAutomatedReasoningPolicyBuildWorkflow",
        "bedrock:getAutomatedReasoningPolicyBuildWorkflowResultAssets",
        "bedrock:getAutomatedReasoningPolicyNextScenario",
        "bedrock:getAutomatedReasoningPolicyTestCase",
        "bedrock:getAutomatedReasoningPolicyTestResult",
```

```
        "bedrock:getBlueprint",
        "bedrock:getCustomModel",
        "bedrock:getCustomModelDeployment",
        "bedrock:getDataAutomationProject",
        "bedrock:getDataAutomationStatus",
        "bedrock:getDataSource",
        "bedrock:getEvaluationJob",
        "bedrock:getExecutionFlowSnapshot",
        "bedrock:getFlow",
        "bedrock:getFlowAlias",
        "bedrock:getFlowExecution",
        "bedrock:getFlowVersion",
        "bedrock:getFoundationModel",
        "bedrock:getFoundationModelAvailability",
        "bedrock:getGuardrail",
        "bedrock:getImportedModel",
        "bedrock:getInferenceProfile",
        "bedrock:getIngestionJob",
        "bedrock:getInvocationStep",
        "bedrock:getKnowledgeBase",
        "bedrock:getMarketplaceModelEndpoint",
        "bedrock:getModelCopyJob",
        "bedrock:getModelCustomizationJob",
        "bedrock:getModelImportJob",
        "bedrock:getModelInvocationJob",
        "bedrock:getModelInvocationLoggingConfiguration",
        "bedrock:getPrompt",
        "bedrock:getPromptRouter",
        "bedrock:getProvisionedModelThroughput",
        "bedrock:getSession",
        "bedrock:getUseCaseForModelAccess",
        "bedrock:listAgentActionGroups",
        "bedrock:listAgentAliases",
        "bedrock:listAgentKnowledgeBases",
        "bedrock:listAgents",
        "bedrock:listAgentVersions",
        "bedrock:listAsyncInvokes",
        "bedrock:listAutomatedReasoningPolicies",
        "bedrock:listAutomatedReasoningPolicyBuildWorkflows",
        "bedrock:listAutomatedReasoningPolicyTestCases",
        "bedrock:listAutomatedReasoningPolicyTestResults",
        "bedrock:listBlueprints",
        "bedrock:listCustomModelDeployments",
        "bedrock:listCustomModels",
```

```
        "bedrock:listDataAutomationProjects",
        "bedrock:listDataSources",
        "bedrock:listEnforcedGuardrailsConfiguration",
        "bedrock:listEvaluationJobs",
        "bedrock:listFlowAliases",
        "bedrock:listFlowExecutionEvents",
        "bedrock:listFlowExecutions",
        "bedrock:listFlows",
        "bedrock:listFlowVersions",
        "bedrock:listFoundationModelAgreementOffers",
        "bedrock:listFoundationModels",
        "bedrock:listGuardrails",
        "bedrock:listImportedModels",
        "bedrock:listInferenceProfiles",
        "bedrock:listIngestionJobs",
        "bedrock:listInvocationSteps",
        "bedrock:listKnowledgeBases",
        "bedrock:listMarketplaceModelEndpoints",
        "bedrock:listModelCopyJobs",
        "bedrock:listModelCustomizationJobs",
        "bedrock:listModelImportJobs",
        "bedrock:listModelInvocationJobs",
        "bedrock:listPromptRouters",
        "bedrock:listPrompts",
        "bedrock:listProvisionedModelThroughputs",
        "bedrock:listSessions",
        "bedrock-agentcore:getAgentCard",
        "bedrock-agentcore:getAgentRuntime",
        "bedrock-agentcore:getAgentRuntimeEndpoint",
        "bedrock-agentcore:getApiKeyCredentialProvider",
        "bedrock-agentcore:getBrowser",
        "bedrock-agentcore:getBrowserProfile",
        "bedrock-agentcore:getBrowserSession",
        "bedrock-agentcore:getCodeInterpreter",
        "bedrock-agentcore:getCodeInterpreterSession",
        "bedrock-agentcore:getConfigurationBundle",
        "bedrock-agentcore:getConfigurationBundleVersion",
        "bedrock-agentcore:getEvaluator",
        "bedrock-agentcore:getEvent",
        "bedrock-agentcore:getGateway",
        "bedrock-agentcore:getGatewayRule",
        "bedrock-agentcore:getGatewayTarget",
        "bedrock-agentcore:getHarness",
        "bedrock-agentcore:getMemory",
```

```
        "bedrock-agentcore:getMemoryRecord",
        "bedrock-agentcore:getOauth2CredentialProvider",
        "bedrock-agentcore:getOnlineEvaluationConfig",
        "bedrock-agentcore:getPaymentConnector",
        "bedrock-agentcore:getPaymentCredentialProvider",
        "bedrock-agentcore:getPaymentManager",
        "bedrock-agentcore:getPolicy",
        "bedrock-agentcore:getPolicyEngine",
        "bedrock-agentcore:getPolicyEngineSummary",
        "bedrock-agentcore:getPolicyGeneration",
        "bedrock-agentcore:getPolicyGenerationSummary",
        "bedrock-agentcore:getPolicySummary",
        "bedrock-agentcore:getRegistry",
        "bedrock-agentcore:getRegistryRecord",
        "bedrock-agentcore:getResourcePolicy",
        "bedrock-agentcore:getTokenVault",
        "bedrock-agentcore:getWorkloadIdentity",
        "bedrock-agentcore:listActors",
        "bedrock-agentcore:listAgentRuntimeEndpoints",
        "bedrock-agentcore:listAgentRuntimeVersions",
        "bedrock-agentcore:listAgentRuntimes",
        "bedrock-agentcore:listApiKeyCredentialProviders",
        "bedrock-agentcore:listBrowserProfiles",
        "bedrock-agentcore:listBrowserSessions",
        "bedrock-agentcore:listBrowsers",
        "bedrock-agentcore:listCodeInterpreterSessions",
        "bedrock-agentcore:listCodeInterpreters",
        "bedrock-agentcore:listConfigurationBundles",
        "bedrock-agentcore:listConfigurationBundleVersions",
        "bedrock-agentcore:listEvaluators",
        "bedrock-agentcore:listEvents",
        "bedrock-agentcore:listGatewayRules",
        "bedrock-agentcore:listGatewayTargets",
        "bedrock-agentcore:listGateways",
        "bedrock-agentcore:listHarnesses",
        "bedrock-agentcore:listMemories",
        "bedrock-agentcore:listMemoryExtractionJobs",
        "bedrock-agentcore:listMemoryRecords",
        "bedrock-agentcore:listOauth2CredentialProviders",
        "bedrock-agentcore:listOnlineEvaluationConfigs",
        "bedrock-agentcore:listPaymentConnectors",
        "bedrock-agentcore:listPaymentCredentialProviders",
        "bedrock-agentcore:listPaymentManagers",
        "bedrock-agentcore:listPolicies",
```

```
        "bedrock-agentcore:listPolicyEngines",
        "bedrock-agentcore:listPolicyEngineSummaries",
        "bedrock-agentcore:listPolicyGenerationAssets",
        "bedrock-agentcore:listPolicyGenerations",
        "bedrock-agentcore:listPolicyGenerationSummaries",
        "bedrock-agentcore:listPolicySummaries",
        "bedrock-agentcore:listRegistries",
        "bedrock-agentcore:listRegistryRecords",
        "bedrock-agentcore:listSessions",
        "bedrock-agentcore:listWorkloadIdentities",
        "braket:getDevice",
        "braket:getJob",
        "braket:getQuantumTask",
        "braket:getServiceLinkedRoleStatus",
        "braket:getUserAgreementStatus",
        "braket:searchDevices",
        "braket:searchJobs",
        "braket:searchQuantumTasks",
        "braket:searchSpendingLimits",
        "budgets:viewBudget",
        "ce:getCostAndUsage",
        "ce:getCostAndUsageWithResources",
        "ce:getCostForecast",
        "ce:getDimensionValues",
        "ce:getReservationCoverage",
        "ce:getReservationPurchaseRecommendation",
        "ce:getReservationUtilization",
        "ce:getRightsizingRecommendation",
        "ce:getSavingsPlansCoverage",
        "ce:getSavingsPlansPurchaseRecommendation",
        "ce:getSavingsPlansUtilization",
        "ce:getSavingsPlansUtilizationDetails",
        "ce:getTags",
        "chatbot:describeChimeWebhookConfigurations",
        "chatbot:describeSlackChannelConfigurations",
        "chatbot:describeSlackUserIdentities",
        "chatbot:describeSlackWorkspaces",
        "chatbot:getMicrosoftTeamsChannelConfiguration",
        "chatbot:listMicrosoftTeamsChannelConfigurations",
        "chatbot:listMicrosoftTeamsConfiguredTeams",
        "chatbot:listMicrosoftTeamsUserIdentities",
        "chime:describeAppInstance",
        "chime:getAttendee",
        "chime:getGlobalSettings",
```

```
        "chime:getMediaCapturePipeline",
        "chime:getMediaPipeline",
        "chime:getMeeting",
        "chime:getProxySession",
        "chime:getSipMediaApplication",
        "chime:getSipRule",
        "chime:getVoiceConnector",
        "chime:getVoiceConnectorGroup",
        "chime:getVoiceConnectorLoggingConfiguration",
        "chime:listAppInstances",
        "chime:listAttendees",
        "chime:listChannelBans",
        "chime:listChannels",
        "chime:listChannelsModeratedByAppInstanceUser",
        "chime:listMediaCapturePipelines",
        "chime:listMediaPipelines",
        "chime:listMeetings",
        "chime:listSipMediaApplications",
        "chime:listSipRules",
        "chime:listVoiceConnectorGroups",
        "chime:listVoiceConnectors",
        "cleanrooms:batchGetCollaborationAnalysisTemplate",
        "cleanrooms:batchGetSchema",
        "cleanrooms:getAnalysisTemplate",
        "cleanrooms:getCollaboration",
        "cleanrooms:getCollaborationAnalysisTemplate",
        "cleanrooms:getCollaborationConfiguredAudienceModelAssociation",
        "cleanrooms:getCollaborationPrivacyBudgetTemplate",
        "cleanrooms:getConfiguredTable",
        "cleanrooms:getConfiguredTableAnalysisRule",
        "cleanrooms:getConfiguredTableAssociation",
        "cleanrooms:getConfiguredAudienceModelAssociation",
        "cleanrooms:getMembership",
        "cleanrooms:getPrivacyBudgetTemplate",
        "cleanrooms:getSchema",
        "cleanrooms:getSchemaAnalysisRule",
        "cleanrooms:listAnalysisTemplates",
        "cleanrooms:listCollaborationAnalysisTemplates",
        "cleanrooms:listCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:listCollaborationPrivacyBudgetTemplates",
        "cleanrooms:listCollaborationPrivacyBudgets",
        "cleanrooms:listCollaborations",
        "cleanrooms:listConfiguredAudienceModelAssociations",
        "cleanrooms:listConfiguredTableAssociations",
```

```
        "cleanrooms:listConfiguredTables",
        "cleanrooms:listMembers",
        "cleanrooms:listMemberships",
        "cleanrooms:listPrivacyBudgetTemplates",
        "cleanrooms:listPrivacyBudgets",
        "cleanrooms:listProtectedQueries",
        "cleanrooms:listSchemas",
        "cleanrooms:previewPrivacyImpact",
        "cloud9:describeEnvironmentMemberships",
        "cloud9:describeEnvironments",
        "cloud9:listEnvironments",
        "clouddirectory:getDirectory",
        "clouddirectory:listDirectories",
        "cloudformation:batchDescribeTypeConfigurations",
        "cloudformation:describeAccountLimits",
        "cloudformation:describeChangeSet",
        "cloudformation:describeChangeSetHooks",
        "cloudformation:describeEvents",
        "cloudformation:describePublisher",
        "cloudformation:describeStackDriftDetectionStatus",
        "cloudformation:describeStackEvents",
        "cloudformation:describeStackInstance",
        "cloudformation:describeStackResource",
        "cloudformation:describeStackResourceDrifts",
        "cloudformation:describeStackResources",
        "cloudformation:describeStacks",
        "cloudformation:describeStackSet",
        "cloudformation:describeStackSetOperation",
        "cloudformation:describeType",
        "cloudformation:describeTypeRegistration",
        "cloudformation:estimateTemplateCost",
        "cloudformation:getResource",
        "cloudformation:getStackPolicy",
        "cloudformation:getTemplate",
        "cloudformation:getTemplateSummary",
        "cloudformation:listChangeSets",
        "cloudformation:listExports",
        "cloudformation:listImports",
        "cloudformation:listResources",
        "cloudformation:listStackInstances",
        "cloudformation:listStackResources",
        "cloudformation:listStacks",
        "cloudformation:listStackSetOperationResults",
        "cloudformation:listStackSetOperations",
```

```
        "cloudformation:listStackSets",
        "cloudformation:listTypeRegistrations",
        "cloudformation:listTypes",
        "cloudformation:listTypeVersions",
        "cloudfront:describeConnectionFunction",
        "cloudfront:describeFunction",
        "cloudfront:describeKeyValueStore",
        "cloudfront:getAnycastIpList",
        "cloudfront:getCachePolicy",
        "cloudfront:getCachePolicyConfig",
        "cloudfront:getCloudFrontOriginAccessIdentity",
        "cloudfront:getCloudFrontOriginAccessIdentityConfig",
        "cloudfront:getConnectionFunction",
        "cloudfront:getConnectionGroup",
        "cloudfront:getConnectionGroupByRoutingEndpoint",
        "cloudfront:getContinuousDeploymentPolicy",
        "cloudfront:getContinuousDeploymentPolicyConfig",
        "cloudfront:getDistribution",
        "cloudfront:getDistributionConfig",
        "cloudfront:getDistributionTenant",
        "cloudfront:getDistributionTenantByDomain",
        "cloudfront:getInvalidation",
        "cloudfront:getInvalidationForDistributionTenant",
        "cloudfront:getKeyGroup",
        "cloudfront:getKeyGroupConfig",
        "cloudfront:getManagedCertificateDetails",
        "cloudfront:getMonitoringSubscription",
        "cloudfront:getOriginAccessControl",
        "cloudfront:getOriginAccessControlConfig",
        "cloudfront:getOriginRequestPolicy",
        "cloudfront:getOriginRequestPolicyConfig",
        "cloudfront:getPublicKey",
        "cloudfront:getPublicKeyConfig",
        "cloudfront:getRealtimeLogConfig",
        "cloudfront:getResourcePolicy",
        "cloudfront:getResponseHeadersPolicy",
        "cloudfront:getResponseHeadersPolicyConfig",
        "cloudfront:getStreamingDistribution",
        "cloudfront:getStreamingDistributionConfig",
        "cloudfront:getTrustStore",
        "cloudfront:getVpcOrigin",
        "cloudfront:listAnycastIpLists",
        "cloudfront:listCachePolicies",
        "cloudfront:listCloudFrontOriginAccessIdentities",
```

```
        "cloudfront:listConnectionFunctions",
        "cloudfront:listConnectionGroups",
        "cloudfront:listConflictingAliases",
        "cloudfront:listContinuousDeploymentPolicies",
        "cloudfront:listDistributions",
        "cloudfront:listDistributionsByAnycastIpListId",
        "cloudfront:listDistributionsByCachePolicyId",
        "cloudfront:listDistributionsByConnectionFunction",
        "cloudfront:listDistributionsByConnectionMode",
        "cloudfront:listDistributionsByKeyGroup",
        "cloudfront:listDistributionsByOriginRequestPolicyId",
        "cloudfront:listDistributionsByRealtimeLogConfig",
        "cloudfront:listDistributionsByResponseHeadersPolicyId",
        "cloudfront:listDistributionsByTrustStore",
        "cloudfront:listDistributionsByVpcOriginId",
        "cloudfront:listDistributionsByWebACLId",
        "cloudfront:listDistributionTenants",
        "cloudfront:listDistributionTenantsByCustomization",
        "cloudfront:listDomainConflicts",
        "cloudfront:listFunctions",
        "cloudfront:listInvalidations",
        "cloudfront:listInvalidationsForDistributionTenant",
        "cloudfront:listKeyGroups",
        "cloudfront:listKeyValueStores",
        "cloudfront:listOriginAccessControls",
        "cloudfront:listOriginRequestPolicies",
        "cloudfront:listPublicKeys",
        "cloudfront:listRealtimeLogConfigs",
        "cloudfront:listResponseHeadersPolicies",
        "cloudfront:listStreamingDistributions",
        "cloudfront:listTagsForResource",
        "cloudfront:listTrustStores",
        "cloudfront:listVpcOrigins",
        "cloudhsm:describeBackups",
        "cloudhsm:describeClusters",
        "cloudsearch:describeAnalysisSchemes",
        "cloudsearch:describeAvailabilityOptions",
        "cloudsearch:describeDomains",
        "cloudsearch:describeExpressions",
        "cloudsearch:describeIndexFields",
        "cloudsearch:describeScalingParameters",
        "cloudsearch:describeServiceAccessPolicies",
        "cloudsearch:describeSuggesters",
        "cloudsearch:listDomainNames",
```

```
        "cloudtrail:describeTrails",
        "cloudtrail:getEventSelectors",
        "cloudtrail:getInsightSelectors",
        "cloudtrail:getTrail",
        "cloudtrail:getTrailStatus",
        "cloudtrail:listEventDataStores",
        "cloudtrail:listPublicKeys",
        "cloudtrail:listTags",
        "cloudtrail:listTrails",
        "cloudtrail:lookupEvents",
        "cloudwatch:describeAlarmHistory",
        "cloudwatch:describeAlarms",
        "cloudwatch:describeAlarmsForMetric",
        "cloudwatch:describeAnomalyDetectors",
        "cloudwatch:describeInsightRules",
        "cloudwatch:getDashboard",
        "cloudwatch:getInsightRuleReport",
        "cloudwatch:getMetricData",
        "cloudwatch:getMetricStatistics",
        "cloudwatch:getMetricStream",
        "cloudWatch:getMetricWidgetImage",
        "cloudwatch:listDashboards",
        "cloudwatch:listManagedInsightRules",
        "cloudwatch:listMetrics",
        "cloudwatch:listMetricStreams",
        "cloudwatch:getAlarmMuteRule",
        "cloudwatch:listAlarmMuteRules",
        "codeartifact:describeDomain",
        "codeartifact:describePackageVersion",
        "codeartifact:describeRepository",
        "codeartifact:getDomainPermissionsPolicy",
        "codeartifact:getRepositoryEndpoint",
        "codeartifact:getRepositoryPermissionsPolicy",
        "codeartifact:listDomains",
        "codeartifact:listPackages",
        "codeartifact:listPackageVersionAssets",
        "codeartifact:listPackageVersions",
        "codeartifact:listRepositories",
        "codeartifact:listRepositoriesInDomain",
        "codebuild:batchGetBuildBatches",
        "codebuild:batchGetBuilds",
        "codebuild:batchGetFleets",
        "codebuild:batchGetProjects",
        "codebuild:listBuildBatches",
```

```
        "codebuild:listBuildBatchesForProject",
        "codebuild:listBuilds",
        "codebuild:listBuildsForProject",
        "codebuild:listCuratedEnvironmentImages",
        "codebuild:listFleets",
        "codebuild:listProjects",
        "codebuild:listSourceCredentials",
        "codecommit:batchGetRepositories",
        "codecommit:getBranch",
        "codecommit:getRepository",
        "codecommit:getRepositoryTriggers",
        "codecommit:listBranches",
        "codecommit:listRepositories",
        "codeconnections:getConnection",
        "codeconnections:getHost",
        "codeconnections:getRepositoryLink",
        "codeconnections:getRepositorySyncStatus",
        "codeconnections:getResourceSyncStatus",
        "codeconnections:getSyncBlockerSummary",
        "codeconnections:getSyncConfiguration",
        "codeconnections:listConnections",
        "codeconnections:listHosts",
        "codeconnections:listRepositoryLinks",
        "codeconnections:listRepositorySyncDefinitions",
        "codeconnections:listSyncConfigurations",
        "codedeploy:batchGetApplicationRevisions",
        "codedeploy:batchGetApplications",
        "codedeploy:batchGetDeploymentGroups",
        "codedeploy:batchGetDeploymentInstances",
        "codedeploy:batchGetDeployments",
        "codedeploy:batchGetDeploymentTargets",
        "codedeploy:batchGetOnPremisesInstances",
        "codedeploy:getApplication",
        "codedeploy:getApplicationRevision",
        "codedeploy:getDeployment",
        "codedeploy:getDeploymentConfig",
        "codedeploy:getDeploymentGroup",
        "codedeploy:getDeploymentInstance",
        "codedeploy:getDeploymentTarget",
        "codedeploy:getOnPremisesInstance",
        "codedeploy:listApplicationRevisions",
        "codedeploy:listApplications",
        "codedeploy:listDeploymentConfigs",
        "codedeploy:listDeploymentGroups",
```

```
        "codedeploy:listDeploymentInstances",
        "codedeploy:listDeployments",
        "codedeploy:listDeploymentTargets",
        "codedeploy:listGitHubAccountTokenNames",
        "codedeploy:listOnPremisesInstances",
        "codepipeline:getJobDetails",
        "codepipeline:getPipeline",
        "codepipeline:getPipelineExecution",
        "codepipeline:getPipelineState",
        "codepipeline:listActionExecutions",
        "codepipeline:listActionTypes",
        "codepipeline:listPipelineExecutions",
        "codepipeline:listPipelines",
        "codepipeline:listRuleExecutions",
        "codepipeline:listWebhooks",
        "codestar-connections:getConnection",
        "codestar-connections:getHost",
        "codestar-connections:listConnections",
        "codestar-connections:listHosts",
        "codestar:describeProject",
        "codestar:listProjects",
        "codestar:listResources",
        "codestar:listTeamMembers",
        "codestar:listUserProfiles",
        "cognito-identity:describeIdentity",
        "cognito-identity:describeIdentityPool",
        "cognito-identity:getIdentityPoolAnalytics",
        "cognito-identity:getIdentityPoolDailyAnalytics",
        "cognito-identity:getIdentityPoolRoles",
        "cognito-identity:getIdentityProviderDailyAnalytics",
        "cognito-identity:listIdentities",
        "cognito-identity:listIdentityPools",
        "cognito-identity:lookupDeveloperIdentity",
        "cognito-idp:describeIdentityProvider",
        "cognito-idp:describeManagedLoginBranding",
        "cognito-idp:describeManagedLoginBrandingByClient",
        "cognito-idp:describeResourceServer",
        "cognito-idp:describeRiskConfiguration",
        "cognito-idp:describeUserImportJob",
        "cognito-idp:describeUserPool",
        "cognito-idp:describeUserPoolClient",
        "cognito-idp:describeUserPoolDomain",
        "cognito-idp:getCSVHeader",
        "cognito-idp:getGroup",
```

```
        "cognito-idp:getLogDeliveryConfiguration",
        "cognito-idp:getUICustomization",
        "cognito-idp:getUserPoolMfaConfig",
        "cognito-idp:getWebACLForResource",
        "cognito-idp:listGroups",
        "cognito-idp:listIdentityProviders",
        "cognito-idp:listResourceServers",
        "cognito-idp:listResourcesForWebACL",
        "cognito-idp:listUserImportJobs",
        "cognito-idp:listUserPoolClients",
        "cognito-idp:listUserPools",
        "cognito-sync:describeDataset",
        "cognito-sync:describeIdentityPoolUsage",
        "cognito-sync:describeIdentityUsage",
        "cognito-sync:getCognitoEvents",
        "cognito-sync:getIdentityPoolConfiguration",
        "cognito-sync:listDatasets",
        "cognito-sync:listIdentityPoolUsage",
        "comprehend:describeDocumentClassificationJob",
        "comprehend:describeDocumentClassifier",
        "comprehend:describeDominantLanguageDetectionJob",
        "comprehend:describeEndpoint",
        "comprehend:describeEntitiesDetectionJob",
        "comprehend:describeEntityRecognizer",
        "comprehend:describeEventsDetectionJob",
        "comprehend:describeFlywheel",
        "comprehend:describeFlywheelIteration",
        "comprehend:describeKeyPhrasesDetectionJob",
        "comprehend:describePiiEntitiesDetectionJob",
        "comprehend:describeSentimentDetectionJob",
        "comprehend:describeTargetedSentimentDetectionJob",
        "comprehend:describeTopicsDetectionJob",
        "comprehend:listDocumentClassificationJobs",
        "comprehend:listDocumentClassifiers",
        "comprehend:listDominantLanguageDetectionJobs",
        "comprehend:listEndpoints",
        "comprehend:listEntitiesDetectionJobs",
        "comprehend:listEntityRecognizers",
        "comprehend:listEventsDetectionJobs",
        "comprehend:listFlywheelIterationHistory",
        "comprehend:listFlywheels",
        "comprehend:listKeyPhrasesDetectionJobs",
        "comprehend:listPiiEntitiesDetectionJobs",
        "comprehend:listSentimentDetectionJobs",
```

```
        "comprehend:listTargetedSentimentDetectionJobs",
        "comprehend:listTopicsDetectionJobs",
        "compute-optimizer:getAutoScalingGroupRecommendations",
        "compute-optimizer:getEBSVolumeRecommendations",
        "compute-optimizer:getEC2InstanceRecommendations",
        "compute-optimizer:getEC2RecommendationProjectedMetrics",
        "compute-optimizer:getECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:getECSServiceRecommendations",
        "compute-optimizer:getEnrollmentStatus",
        "compute-optimizer:getIdleRecommendations",
        "compute-optimizer:getRDSDatabaseRecommendationProjectedMetrics",
        "compute-optimizer:getRDSDatabaseRecommendations",
        "compute-optimizer:getRecommendationSummaries",
        "config:batchGetAggregateResourceConfig",
        "config:batchGetResourceConfig",
        "config:describeAggregateComplianceByConfigRules",
        "config:describeAggregationAuthorizations",
        "config:describeComplianceByConfigRule",
        "config:describeComplianceByResource",
        "config:describeConfigRuleEvaluationStatus",
        "config:describeConfigRules",
        "config:describeConfigurationAggregators",
        "config:describeConfigurationAggregatorSourcesStatus",
        "config:describeConfigurationRecorders",
        "config:describeConfigurationRecorderStatus",
        "config:describeConformancePackCompliance",
        "config:describeConformancePacks",
        "config:describeConformancePackStatus",
        "config:describeDeliveryChannels",
        "config:describeDeliveryChannelStatus",
        "config:describeOrganizationConfigRules",
        "config:describeOrganizationConfigRuleStatuses",
        "config:describeOrganizationConformancePacks",
        "config:describeOrganizationConformancePackStatuses",
        "config:describePendingAggregationRequests",
        "config:describeRemediationConfigurations",
        "config:describeRemediationExceptions",
        "config:describeRemediationExecutionStatus",
        "config:describeRetentionConfigurations",
        "config:getAggregateComplianceDetailsByConfigRule",
        "config:getAggregateConfigRuleComplianceSummary",
        "config:getAggregateDiscoveredResourceCounts",
        "config:getAggregateResourceConfig",
        "config:getComplianceDetailsByConfigRule",
```

```
        "config:getComplianceDetailsByResource",
        "config:getComplianceSummaryByConfigRule",
        "config:getComplianceSummaryByResourceType",
        "config:getConformancePackComplianceDetails",
        "config:getConformancePackComplianceSummary",
        "config:getDiscoveredResourceCounts",
        "config:getOrganizationConfigRuleDetailedStatus",
        "config:getOrganizationConformancePackDetailedStatus",
        "config:getResourceConfigHistory",
        "config:listAggregateDiscoveredResources",
        "config:listDiscoveredResources",
        "config:listTagsForResource",
        "config:selectAggregateResourceConfig",
        "config:selectResourceConfig",
        "connect:batchGetFlowAssociation",
        "connect:describeContact",
        "connect:describeContactFlow",
        "connect:describeInstance",
        "connect:describeInstanceAttribute",
        "connect:describePhoneNumber",
        "connect:describeQueue",
        "connect:describeQuickConnect",
        "connect:describeRoutingProfile",
        "connect:describeUser",
        "connect:describeUserHierarchyStructure",
        "connect:getCurrentMetricData",
        "connect:getMetricData",
        "connect:getMetricDataV2",
        "connect:listContactEvaluations",
        "connect:listEvaluationForms",
        "connect:listEvaluationFormVersions",
        "connect:listInstanceAttributes",
        "connect:listInstanceStorageConfigs",
        "connect:listPhoneNumbersV2",
        "connect:listQueueQuickConnects",
        "connect:listQueues",
        "connect:listQuickConnects",
        "connect:listRoutingProfileQueues",
        "connect:listRoutingProfiles",
        "connect:listSecurityProfiles",
        "connect:listSecurityProfilePermissions",
        "connect:listUsers",
        "connect:listViews",
        "connect:listViewVersions",
```

```
        "connect:searchQueues",
        "connect:searchRoutingProfiles",
        "connect:searchUsers",
        "connect-campaigns:describeCampaign",
        "controlcatalog:getControl",
        "controltower:describeAccountFactoryConfig",
        "controltower:describeCoreService",
        "controltower:describeGuardrail",
        "controltower:describeGuardrailForTarget",
        "controltower:describeManagedAccount",
        "controltower:describeSingleSignOn",
        "controltower:getAvailableUpdates",
        "controltower:getBaselineOperation",
        "controltower:getControlOperation",
        "controltower:getEnabledBaseline",
        "controltower:getEnabledControl",
        "controltower:getHomeRegion",
        "controltower:getLandingZone",
        "controltower:getLandingZoneStatus",
        "controltower:listBaselines",
        "controltower:listDirectoryGroups",
        "controltower:listEnabledControls",
        "controltower:listEnabledBaselines",
        "controltower:listGuardrailsForTarget",
        "controltower:listGuardrailViolations",
        "controltower:listLandingZones",
        "controltower:listManagedAccounts",
        "controltower:listManagedAccountsForGuardrail",
        "controltower:listManagedAccountsForParent",
        "controltower:listManagedOrganizationalUnits",
        "controltower:listManagedOrganizationalUnitsForGuardrail",
        "cost-optimization-hub:getPreferences",
        "cost-optimization-hub:getRecommendation",
        "cost-optimization-hub:listEnrollmentStatuses",
        "cost-optimization-hub:listRecommendations",
        "cost-optimization-hub:listRecommendationSummaries",
        "databrew:describeDataset",
        "databrew:describeJob",
        "databrew:describeProject",
        "databrew:describeRecipe",
        "databrew:listDatasets",
        "databrew:listJobRuns",
        "databrew:listJobs",
        "databrew:listProjects",
```

```
        "databrew:listRecipes",
        "databrew:listRecipeVersions",
        "databrew:listTagsForResource",
        "datapipeline:describeObjects",
        "datapipeline:describePipelines",
        "datapipeline:getPipelineDefinition",
        "datapipeline:listPipelines",
        "datapipeline:queryObjects",
        "datasync:describeAgent",
        "datasync:describeLocationAzureBlob",
        "datasync:describeLocationEfs",
        "datasync:describeLocationFsxLustre",
        "datasync:describeLocationFsxOntap",
        "datasync:describeLocationFsxOpenZfs",
        "datasync:describeLocationFsxWindows",
        "datasync:describeLocationHdfs",
        "datasync:describeLocationNfs",
        "datasync:describeLocationObjectStorage",
        "datasync:describeLocationS3",
        "datasync:describeLocationSmb",
        "datasync:describeTask",
        "datasync:describeTaskExecution",
        "datasync:listAgents",
        "datasync:listLocations",
        "datasync:listTaskExecutions",
        "datasync:listTasks",
        "datazone:getAsset",
        "datazone:getAssetType",
        "datazone:getDataSource",
        "datazone:getDataSourceRun",
        "datazone:getDomain",
        "datazone:getEnvironment",
        "datazone:getEnvironmentBlueprint",
        "datazone:getEnvironmentBlueprintConfiguration",
        "datazone:getEnvironmentProfile",
        "datazone:getFormType",
        "datazone:getGlossary",
        "datazone:getGlossaryTerm",
        "datazone:getGroupProfile",
        "datazone:getListing",
        "datazone:getMetadataGenerationRun",
        "datazone:getProject",
        "datazone:getSubscription",
        "datazone:getSubscriptionGrant",
```

```
        "datazone:getSubscriptionRequestDetails",
        "datazone:getSubscriptionTarget",
        "datazone:getUserProfile",
        "datazone:listAssetRevisions",
        "datazone:listDataSourceRunActivities",
        "datazone:listDataSourceRuns",
        "datazone:listDataSources",
        "datazone:listDomains",
        "datazone:listEnvironmentBlueprintConfigurations",
        "datazone:listEnvironmentBlueprints",
        "datazone:listEnvironmentProfiles",
        "datazone:listEnvironments",
        "datazone:listMetadataGenerationRuns",
        "datazone:listProjectMemberships",
        "datazone:listProjects",
        "datazone:listSubscriptionGrants",
        "datazone:listSubscriptionRequests",
        "datazone:listSubscriptions",
        "datazone:listSubscriptionTargets",
        "datazone:getAssetFilter",
        "datazone:getDomainUnit",
        "datazone:getLineageNode",
        "datazone:getProjectProfile",
        "datazone:getRule",
        "datazone:listAssetFilters",
        "datazone:listConnections",
        "datazone:listDomainUnitsForParent",
        "datazone:listEntityOwners",
        "datazone:listLineageNodeHistory",
        "datazone:listNotifications",
        "datazone:listPolicyGrants",
        "datazone:listProjectProfiles",
        "datazone:listRules",
        "datazone:searchGroupProfiles",
        "datazone:searchUserProfiles",
        "dax:describeClusters",
        "dax:describeDefaultParameters",
        "dax:describeEvents",
        "dax:describeParameterGroups",
        "dax:describeParameters",
        "dax:describeSubnetGroups",
        "deadline:listAvailableMeteredProducts",
        "deadline:listBudgets",
        "deadline:listFarmMembers",
```

```
        "deadline:listFarms",
        "deadline:listFleetMembers",
        "deadline:listFleets",
        "deadline:listJobMembers",
        "deadline:listJobs",
        "deadline:listLicenseEndpoints",
        "deadline:listMeteredProducts",
        "deadline:listMonitors",
        "deadline:listQueueEnvironments",
        "deadline:listQueueFleetAssociations",
        "deadline:listQueueMembers",
        "deadline:listQueues",
        "deadline:listStorageProfiles",
        "deadline:listWorkers",
        "detective:getMembers",
        "detective:listGraphs",
        "detective:listInvitations",
        "detective:listMembers",
        "devicefarm:getAccountSettings",
        "devicefarm:getDevice",
        "devicefarm:getDevicePool",
        "devicefarm:getDevicePoolCompatibility",
        "devicefarm:getJob",
        "devicefarm:getOfferingStatus",
        "devicefarm:getProject",
        "devicefarm:getRemoteAccessSession",
        "devicefarm:getRun",
        "devicefarm:getSuite",
        "devicefarm:getTest",
        "devicefarm:getTestGridProject",
        "devicefarm:getTestGridSession",
        "devicefarm:getUpload",
        "devicefarm:getVPCEConfiguration",
        "devicefarm:listArtifacts",
        "devicefarm:listDevicePools",
        "devicefarm:listDevices",
        "devicefarm:listJobs",
        "devicefarm:listNetworkProfiles",
        "devicefarm:listOfferingPromotions",
        "devicefarm:listOfferingTransactions",
        "devicefarm:listProjects",
        "devicefarm:listRemoteAccessSessions",
        "devicefarm:listRuns",
        "devicefarm:listSamples",
```

```
        "devicefarm:listSuites",
        "devicefarm:listTestGridProjects",
        "devicefarm:listTestGridSessionActions",
        "devicefarm:listTestGridSessionArtifacts",
        "devicefarm:listTestGridSessions",
        "devicefarm:listTests",
        "devicefarm:listUniqueProblems",
        "devicefarm:listUploads",
        "devicefarm:listVPCEConfigurations",
        "directconnect:describeConnectionLoa",
        "directconnect:describeConnections",
        "directconnect:describeConnectionsOnInterconnect",
        "directconnect:describeCustomerMetadata",
        "directconnect:describeDirectConnectGatewayAssociationProposals",
        "directconnect:describeDirectConnectGatewayAssociations",
        "directconnect:describeDirectConnectGatewayAttachments",
        "directconnect:describeDirectConnectGateways",
        "directconnect:describeHostedConnections",
        "directconnect:describeInterconnectLoa",
        "directconnect:describeInterconnects",
        "directconnect:describeLags",
        "directconnect:describeLoa",
        "directconnect:describeLocations",
        "directconnect:describeRouterConfiguration",
        "directconnect:describeVirtualGateways",
        "directconnect:describeVirtualInterfaces",
        "directconnect:listVirtualInterfaceTestHistory",
        "dlm:getLifecyclePolicies",
        "dlm:getLifecyclePolicy",
        "dms:describeAccountAttributes",
        "dms:describeApplicableIndividualAssessments",
        "dms:describeCertificates",
        "dms:describeConnections",
        "dms:describeEndpoints",
        "dms:describeEndpointSettings",
        "dms:describeEndpointTypes",
        "dms:describeEventCategories",
        "dms:describeEvents",
        "dms:describeEventSubscriptions",
        "dms:describeFleetAdvisorCollectors",
        "dms:describeFleetAdvisorDatabases",
        "dms:describeFleetAdvisorLsaAnalysis",
        "dms:describeFleetAdvisorSchemaObjectSummary",
        "dms:describeFleetAdvisorSchemas",
```

```
        "dms:describeOrderableReplicationInstances",
        "dms:describePendingMaintenanceActions",
        "dms:describeRefreshSchemasStatus",
        "dms:describeReplicationConfigs",
        "dms:describeReplicationInstances",
        "dms:describeReplicationInstanceTaskLogs",
        "dms:describeReplications",
        "dms:describeReplicationSubnetGroups",
        "dms:describeReplicationTableStatistics",
        "dms:describeReplicationTaskAssessmentResults",
        "dms:describeReplicationTaskAssessmentRuns",
        "dms:describeReplicationTaskIndividualAssessments",
        "dms:describeReplicationTasks",
        "dms:describeSchemas",
        "dms:describeTableStatistics",
        "docdb-elastic:getCluster",
        "docdb-elastic:getClusterSnapshot",
        "docdb-elastic:listClusters",
        "docdb-elastic:listClusterSnapshots",
        "drs:describeJobLogItems",
        "drs:describeJobs",
        "drs:describeLaunchConfigurationTemplates",
        "drs:describeRecoveryInstances",
        "drs:describeRecoverySnapshots",
        "drs:describeReplicationConfigurationTemplates",
        "drs:describeSourceNetworks",
        "drs:describeSourceServers",
        "drs:getLaunchConfiguration",
        "drs:getReplicationConfiguration",
        "drs:listExtensibleSourceServers",
        "drs:listLaunchActions",
        "drs:listStagingAccounts",
        "ds:describeClientAuthenticationSettings",
        "ds:describeConditionalForwarders",
        "ds:describeDirectories",
        "ds:describeDomainControllers",
        "ds:describeEventTopics",
        "ds:describeHybridADUpdate",
        "ds:describeLDAPSSettings",
        "ds:describeSharedDirectories",
        "ds:describeSnapshots",
        "ds:describeTrusts",
        "ds:getDirectoryLimits",
        "ds:getSnapshotLimits",
```

```
        "ds:listIpRoutes",
        "ds:listSchemaExtensions",
        "ds:listTagsForResource",
        "dsql:getCluster",
        "dsql:getVpcEndpointServiceName",
        "dsql:listClusters",
        "dynamodb:describeBackup",
        "dynamodb:describeContinuousBackups",
        "dynamodb:describeContributorInsights",
        "dynamodb:describeExport",
        "dynamodb:describeGlobalTable",
        "dynamodb:describeGlobalTableSettings",
        "dynamodb:describeImport",
        "dynamodb:describeKinesisStreamingDestination",
        "dynamodb:describeLimits",
        "dynamodb:describeStream",
        "dynamodb:describeTable",
        "dynamodb:describeTableReplicaAutoScaling",
        "dynamodb:describeTimeToLive",
        "dynamodb:getResourcePolicy",
        "dynamodb:listBackups",
        "dynamodb:listContributorInsights",
        "dynamodb:listExports",
        "dynamodb:listGlobalTables",
        "dynamodb:listImports",
        "dynamodb:listStreams",
        "dynamodb:listTables",
        "dynamodb:listTagsOfResource",
        "ebs:listChangedBlocks",
        "ebs:listSnapshotBlocks",
        "ec2:describeAccountAttributes",
        "ec2:describeAddresses",
        "ec2:describeAddressesAttribute",
        "ec2:describeAddressTransfers",
        "ec2:describeAggregateIdFormat",
        "ec2:describeAvailabilityZones",
        "ec2:describeBundleTasks",
        "ec2:describeByoipCidrs",
        "ec2:describeCapacityBlockOfferings",
        "ec2:describeCapacityBlocks",
        "ec2:describeCapacityBlockStatus",
        "ec2:describeCapacityManagerDataExports",
        "ec2:describeCapacityReservationFleets",
        "ec2:describeCapacityReservations",
```

```
        "ec2:describeCapacityReservationTopology",
        "ec2:describeCarrierGateways",
        "ec2:describeClassicLinkInstances",
        "ec2:describeClientVpnAuthorizationRules",
        "ec2:describeClientVpnConnections",
        "ec2:describeClientVpnEndpoints",
        "ec2:describeClientVpnRoutes",
        "ec2:describeClientVpnTargetNetworks",
        "ec2:describeCoipPools",
        "ec2:describeConversionTasks",
        "ec2:describeCustomerGateways",
        "ec2:describeDhcpOptions",
        "ec2:describeEgressOnlyInternetGateways",
        "ec2:describeExportImageTasks",
        "ec2:describeExportTasks",
        "ec2:describeFastLaunchImages",
        "ec2:describeFastSnapshotRestores",
        "ec2:describeFleetHistory",
        "ec2:describeFleetInstances",
        "ec2:describeFleets",
        "ec2:describeFlowLogs",
        "ec2:describeFpgaImageAttribute",
        "ec2:describeFpgaImages",
        "ec2:describeHostReservationOfferings",
        "ec2:describeHostReservations",
        "ec2:describeHosts",
        "ec2:describeIamInstanceProfileAssociations",
        "ec2:describeIdentityIdFormat",
        "ec2:describeIdFormat",
        "ec2:describeImageAttribute",
        "ec2:describeImages",
        "ec2:describeImportImageTasks",
        "ec2:describeImportSnapshotTasks",
        "ec2:describeInstanceAttribute",
        "ec2:describeInstanceConnectEndpoints",
        "ec2:describeInstanceCreditSpecifications",
        "ec2:describeInstanceEventNotificationAttributes",
        "ec2:describeInstanceEventWindows",
        "ec2:describeInstances",
        "ec2:describeInstanceStatus",
        "ec2:describeInstanceTypeOfferings",
        "ec2:describeInstanceTypes",
        "ec2:describeInstanceTopology",
        "ec2:describeInternetGateways",
```

```
        "ec2:describeIpamByoasn",
        "ec2:describeIpamExternalResourceVerificationTokens",
        "ec2:describeIpamPools",
        "ec2:describeIpamResourceDiscoveries",
        "ec2:describeIpamResourceDiscoveryAssociations",
        "ec2:describeIpams",
        "ec2:describeIpamScopes",
        "ec2:describeIpv6Pools",
        "ec2:describeKeyPairs",
        "ec2:describeLaunchTemplates",
        "ec2:describeLaunchTemplateVersions",
        "ec2:describeLocalGatewayRouteTables",
        "ec2:describeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:describeLocalGatewayRouteTableVpcAssociations",
        "ec2:describeLocalGateways",
        "ec2:describeLocalGatewayVirtualInterfaceGroups",
        "ec2:describeLocalGatewayVirtualInterfaces",
        "ec2:describeManagedPrefixLists",
        "ec2:describeMovingAddresses",
        "ec2:describeNatGateways",
        "ec2:describeNetworkAcls",
        "ec2:describeNetworkInsightsAccessScopeAnalyses",
        "ec2:describeNetworkInsightsAccessScopes",
        "ec2:describeNetworkInsightsAnalyses",
        "ec2:describeNetworkInsightsPaths",
        "ec2:describeNetworkInterfaceAttribute",
        "ec2:describeNetworkInterfaces",
        "ec2:describeOutpostLags",
        "ec2:describePlacementGroups",
        "ec2:describePrefixLists",
        "ec2:describePrincipalIdFormat",
        "ec2:describePublicIpv4Pools",
        "ec2:describeRegions",
        "ec2:describeReplaceRootVolumeTasks",
        "ec2:describeReservedInstances",
        "ec2:describeReservedInstancesListings",
        "ec2:describeReservedInstancesModifications",
        "ec2:describeReservedInstancesOfferings",
        "ec2:describeRouteServerEndpoints",
        "ec2:describeRouteServerPeers",
        "ec2:describeRouteServers",
        "ec2:describeRouteTables",
        "ec2:describeScheduledInstanceAvailability",
        "ec2:describeScheduledInstances",
```

```
        "ec2:describeSecurityGroupReferences",
        "ec2:describeSecurityGroupRules",
        "ec2:describeSecurityGroups",
        "ec2:describeServiceLinkVirtualInterfaces",
        "ec2:describeSnapshotAttribute",
        "ec2:describeSnapshots",
        "ec2:describeSnapshotTierStatus",
        "ec2:describeSpotDatafeedSubscription",
        "ec2:describeSpotFleetInstances",
        "ec2:describeSpotFleetRequestHistory",
        "ec2:describeSpotFleetRequests",
        "ec2:describeSpotInstanceRequests",
        "ec2:describeSpotPriceHistory",
        "ec2:describeStaleSecurityGroups",
        "ec2:describeStoreImageTasks",
        "ec2:describeSubnets",
        "ec2:describeTags",
        "ec2:describeTrafficMirrorFilterRules",
        "ec2:describeTrafficMirrorFilters",
        "ec2:describeTrafficMirrorSessions",
        "ec2:describeTrafficMirrorTargets",
        "ec2:describeTransitGatewayAttachments",
        "ec2:describeTransitGatewayConnectPeers",
        "ec2:describeTransitGatewayConnects",
        "ec2:describeTransitGatewayMeteringPolicies",
        "ec2:describeTransitGatewayMulticastDomains",
        "ec2:describeTransitGatewayPeeringAttachments",
        "ec2:describeTransitGatewayPolicyTables",
        "ec2:describeTransitGatewayRouteTableAnnouncements",
        "ec2:describeTransitGatewayRouteTables",
        "ec2:describeTransitGateways",
        "ec2:describeTransitGatewayVpcAttachments",
        "ec2:describeVerifiedAccessEndpoints",
        "ec2:describeVerifiedAccessGroups",
        "ec2:describeVerifiedAccessInstanceLoggingConfigurations",
        "ec2:describeVerifiedAccessInstances",
        "ec2:describeVerifiedAccessInstanceWebAclAssociations",
        "ec2:describeVerifiedAccessTrustProviders",
        "ec2:describeVolumeAttribute",
        "ec2:describeVolumes",
        "ec2:describeVolumesModifications",
        "ec2:describeVolumeStatus",
        "ec2:describeVpcAttribute",
        "ec2:describeVpcBlockPublicAccessExclusions",
```

```
        "ec2:describeVpcBlockPublicAccessOptions",
        "ec2:describeVpcClassicLink",
        "ec2:describeVpcClassicLinkDnsSupport",
        "ec2:describeVpcEndpointAssociations",
        "ec2:describeVpcEndpointConnectionNotifications",
        "ec2:describeVpcEndpointConnections",
        "ec2:describeVpcEndpoints",
        "ec2:describeVpcEndpointServiceConfigurations",
        "ec2:describeVpcEndpointServicePermissions",
        "ec2:describeVpcEndpointServices",
        "ec2:describeVpcEncryptionControls",
        "ec2:describeVpcPeeringConnections",
        "ec2:describeVpcs",
        "ec2:describeVpnConnections",
        "ec2:describeVpnGateways",
        "ec2:getAssociatedEnclaveCertificateIamRoles",
        "ec2:getAssociatedIpv6PoolCidrs",
        "ec2:getCapacityManagerAttributes",
        "ec2:getCapacityManagerMetricData",
        "ec2:getCapacityManagerMetricDimensions",
        "ec2:getCapacityReservationUsage",
        "ec2:getCoipPoolUsage",
        "ec2:getConsoleOutput",
        "ec2:getConsoleScreenshot",
        "ec2:getDefaultCreditSpecification",
        "ec2:getEbsDefaultKmsKeyId",
        "ec2:getEbsEncryptionByDefault",
        "ec2:getGroupsForCapacityReservation",
        "ec2:getHostReservationPurchasePreview",
        "ec2:getImageBlockPublicAccessState",
        "ec2:getInstanceTypesFromInstanceRequirements",
        "ec2:getIpamAddressHistory",
        "ec2:getIpamDiscoveredAccounts",
        "ec2:getIpamDiscoveredPublicAddresses",
        "ec2:getIpamDiscoveredResourceCidrs",
        "ec2:getIpamPoolAllocations",
        "ec2:getIpamPoolCidrs",
        "ec2:getIpamResourceCidrs",
        "ec2:getLaunchTemplateData",
        "ec2:getManagedPrefixListAssociations",
        "ec2:getManagedPrefixListEntries",
        "ec2:getNetworkInsightsAccessScopeContent",
        "ec2:getReservedInstancesExchangeQuote",
        "ec2:getRouteServerAssociations",
```

```
        "ec2:getRouteServerPropagations",
        "ec2:getRouteServerRoutingDatabase",
        "ec2:getSerialConsoleAccessStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSSupportActionsGroup2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:getSpotPlacementScores",
        "ec2:getSubnetCidrReservations",
        "ec2:getTransitGatewayAttachmentPropagations",
        "ec2:getTransitGatewayMulticastDomainAssociations",
        "ec2:getTransitGatewayPolicyTableAssociations",
        "ec2:getTransitGatewayPolicyTableEntries",
        "ec2:getTransitGatewayPrefixListReferences",
        "ec2:getTransitGatewayRouteTableAssociations",
        "ec2:getTransitGatewayRouteTablePropagations",
        "ec2:getVerifiedAccessEndpointPolicy",
        "ec2:getVerifiedAccessGroupPolicy",
        "ec2:getVpcResourcesBlockingEncryptionEnforcement",
        "ec2:getVpnTunnelReplacementStatus",
        "ec2:listImagesInRecycleBin",
        "ec2:listSnapshotsInRecycleBin",
        "ec2:searchLocalGatewayRoutes",
        "ec2:searchTransitGatewayMulticastGroups",
        "ec2:searchTransitGatewayRoutes",
        "ecr-public:describeImages",
        "ecr-public:describeImageTags",
        "ecr-public:describeRegistries",
        "ecr-public:describeRepositories",
        "ecr-public:getRegistryCatalogData",
        "ecr-public:getRepositoryCatalogData",
        "ecr-public:getRepositoryPolicy",
        "ecr-public:listTagsForResource",
        "ecr:batchCheckLayerAvailability",
        "ecr:batchGetImage",
        "ecr:batchGetRepositoryScanningConfiguration",
        "ecr:describeImageReplicationStatus",
        "ecr:describeImages",
        "ecr:describeImageScanFindings",
```

```
        "ecr:describeImageSigningStatus",
        "ecr:describePullThroughCacheRules",
        "ecr:describeRegistry",
        "ecr:describeRepositories",
        "ecr:describeRepositoryCreationTemplates",
        "ecr:getAccountSetting",
        "ecr:getAuthorizationToken",
        "ecr:getDownloadUrlForLayer",
        "ecr:getLifecyclePolicy",
        "ecr:getLifecyclePolicyPreview",
        "ecr:getRegistryPolicy",
        "ecr:getRegistryScanningConfiguration",
        "ecr:getRepositoryPolicy",
        "ecr:getSigningConfiguration",
        "ecr:listImages",
        "ecr:listPullTimeUpdateExclusions",
        "ecr:listTagsForResource",
        "ecs:describeCapacityProviders",
        "ecs:describeClusters",
        "ecs:describeContainerInstances",
        "ecs:describeExpressGatewayService",
        "ecs:describeServiceDeployments",
        "ecs:describeServiceRevisions",
        "ecs:describeServices",
        "ecs:describeTaskDefinition",
        "ecs:describeTasks",
        "ecs:describeTaskSets",
        "ecs:getTaskProtection",
        "ecs:listAccountSettings",
        "ecs:listAttributes",
        "ecs:listClusters",
        "ecs:listContainerInstances",
        "ecs:listServiceDeployments",
        "ecs:listServices",
        "ecs:listServicesByNamespace",
        "ecs:listTagsForResource",
        "ecs:listTaskDefinitionFamilies",
        "ecs:listTaskDefinitions",
        "ecs:listTasks",
        "eks:describeAccessEntry",
        "eks:describeAddon",
        "eks:describeAddonConfiguration",
        "eks:describeAddonVersions",
        "eks:describeCapability",
```

```
        "eks:describeCluster",
        "eks:describeClusterVersions",
        "eks:describeEksAnywhereSubscription",
        "eks:describeFargateProfile",
        "eks:describeIdentityProviderConfig",
        "eks:describeInsight",
        "eks:describeNodegroup",
        "eks:describePodIdentityAssociation",
        "eks:describeUpdate",
        "eks:listAccessEntries",
        "eks:listAccessPolicies",
        "eks:listAddons",
        "eks:listAssociatedAccessPolicies",
        "eks:listCapabilities",
        "eks:listClusters",
        "eks:listEksAnywhereSubscriptions",
        "eks:listFargateProfiles",
        "eks:listIdentityProviderConfigs",
        "eks:listInsights",
        "eks:listNodegroups",
        "eks:listPodIdentityAssociations",
        "eks:listUpdates",
        "elasticache:describeCacheClusters",
        "elasticache:describeCacheEngineVersions",
        "elasticache:describeCacheParameterGroups",
        "elasticache:describeCacheParameters",
        "elasticache:describeCacheSecurityGroups",
        "elasticache:describeCacheSubnetGroups",
        "elasticache:describeEngineDefaultParameters",
        "elasticache:describeEvents",
        "elasticache:describeGlobalReplicationGroups",
        "elasticache:describeReplicationGroups",
        "elasticache:describeReservedCacheNodes",
        "elasticache:describeReservedCacheNodesOfferings",
        "elasticache:describeServerlessCaches",
        "elasticache:describeServerlessCacheSnapshots",
        "elasticache:describeServiceUpdates",
        "elasticache:describeSnapshots",
        "elasticache:describeUpdateActions",
        "elasticache:describeUserGroups",
        "elasticache:describeUsers",
        "elasticache:listAllowedNodeTypeModifications",
        "elasticache:listTagsForResource",
        "elasticbeanstalk:checkDNSAvailability",
```

```
        "elasticbeanstalk:describeAccountAttributes",
        "elasticbeanstalk:describeApplications",
        "elasticbeanstalk:describeApplicationVersions",
        "elasticbeanstalk:describeConfigurationOptions",
        "elasticbeanstalk:describeEnvironmentHealth",
        "elasticbeanstalk:describeEnvironmentManagedActionHistory",
        "elasticbeanstalk:describeEnvironmentManagedActions",
        "elasticbeanstalk:describeEnvironmentResources",
        "elasticbeanstalk:describeEnvironments",
        "elasticbeanstalk:describeEvents",
        "elasticbeanstalk:describeInstancesHealth",
        "elasticbeanstalk:describePlatformVersion",
        "elasticbeanstalk:listAvailableSolutionStacks",
        "elasticbeanstalk:listPlatformBranches",
        "elasticbeanstalk:listPlatformVersions",
        "elasticbeanstalk:listTagsForResource",
        "elasticbeanstalk:describeConfigurationSettings",
        "elasticbeanstalk:validateConfigurationSettings",
        "elasticfilesystem:describeAccessPoints",
        "elasticfilesystem:describeBackupPolicy",
        "elasticfilesystem:describeFileSystemPolicy",
        "elasticfilesystem:describeFileSystems",
        "elasticfilesystem:describeLifecycleConfiguration",
        "elasticfilesystem:describeMountTargets",
        "elasticfilesystem:describeMountTargetSecurityGroups",
        "elasticfilesystem:describeReplicationConfigurations",
        "elasticfilesystem:describeTags",
        "elasticfilesystem:listTagsForResource",
        "elasticloadbalancing:describeAccountLimits",
        "elasticloadbalancing:describeInstanceHealth",
        "elasticloadbalancing:describeListenerCertificates",
        "elasticloadbalancing:describeListeners",
        "elasticloadbalancing:describeLoadBalancerAttributes",
        "elasticloadbalancing:describeLoadBalancerPolicies",
        "elasticloadbalancing:describeLoadBalancerPolicyTypes",
        "elasticloadbalancing:describeLoadBalancers",
        "elasticloadbalancing:describeRules",
        "elasticloadbalancing:describeSSLPolicies",
        "elasticloadbalancing:describeTags",
        "elasticloadbalancing:describeTargetGroupAttributes",
        "elasticloadbalancing:describeTargetGroups",
        "elasticloadbalancing:describeTargetHealth",
        "elasticloadbalancing:describeTrustStoreAssociations",
        "elasticloadbalancing:describeTrustStoreRevocations",
```

```
        "elasticloadbalancing:describeTrustStores",
        "elasticmapreduce:describeCluster",
        "elasticmapreduce:describeNotebookExecution",
        "elasticmapreduce:describePersistentAppUI",
        "elasticmapreduce:describeReleaseLabel",
        "elasticmapreduce:describeSecurityConfiguration",
        "elasticmapreduce:describeStep",
        "elasticmapreduce:describeStudio",
        "elasticmapreduce:getAutoTerminationPolicy",
        "elasticmapreduce:getBlockPublicAccessConfiguration",
        "elasticmapreduce:getManagedScalingPolicy",
        "elasticmapreduce:getStudioSessionMapping",
        "elasticmapreduce:listBootstrapActions",
        "elasticmapreduce:listClusters",
        "elasticmapreduce:listInstanceFleets",
        "elasticmapreduce:listInstanceGroups",
        "elasticmapreduce:listInstances",
        "elasticmapreduce:listNotebookExecutions",
        "elasticmapreduce:listReleaseLabels",
        "elasticmapreduce:listSecurityConfigurations",
        "elasticmapreduce:listSteps",
        "elasticmapreduce:listStudios",
        "elasticmapreduce:listStudioSessionMappings",
        "elasticmapreduce:listSupportedInstanceTypes",
        "emr-containers:describeJobRun",
        "emr-containers:describeJobTemplate",
        "emr-containers:describeManagedEndpoint",
        "emr-containers:describeVirtualCluster",
        "emr-containers:listJobRuns",
        "emr-containers:listJobTemplates",
        "emr-containers:listManagedEndpoints",
        "emr-containers:listVirtualClusters",
        "emr-serverless:getApplication",
        "emr-serverless:getJobRun",
        "emr-serverless:listApplications",
        "emr-serverless:listJobRunAttempts",
        "emr-serverless:listJobRuns",
        "entityresolution:getIdMappingJob",
        "entityresolution:getIdMappingWorkflow",
        "entityresolution:getMatchingJob",
        "entityresolution:getMatchingWorkflow",
        "entityresolution:getProviderService",
        "entityresolution:getSchemaMapping",
        "entityresolution:listIdMappingJobs",
```

```
        "entityresolution:listIdMappingWorkflows",
        "entityresolution:listMatchingJobs",
        "entityresolution:listMatchingWorkflows",
        "entityresolution:listProviderServices",
        "entityresolution:listSchemaMappings",
        "es:describeDomain",
        "es:describeDomainAutoTunes",
        "es:describeDomainChangeProgress",
        "es:describeDomainConfig",
        "es:describeDomainHealth",
        "es:describeDomainNodes",
        "es:describeDomains",
        "es:describeDryRunProgress",
        "es:describeElasticsearchDomain",
        "es:describeElasticsearchDomainConfig",
        "es:describeElasticsearchDomains",
        "es:getApplication",
        "es:getCapability",
        "es:getDataSource",
        "es:getDefaultApplicationSetting",
        "es:getDirectQueryDataSource",
        "es:getDomainMaintenanceStatus",
        "es:describeInboundConnections",
        "es:describeInstanceTypeLimits",
        "es:describeInsightDetails",
        "es:describeOutboundConnections",
        "es:describePackages",
        "es:describeReservedInstanceOfferings",
        "es:describeReservedInstances",
        "es:describeVpcEndpoints",
        "es:getCompatibleVersions",
        "es:getPackageVersionHistory",
        "es:getUpgradeHistory",
        "es:getUpgradeStatus",
        "es:listApplications",
        "es:listDataSources",
        "es:listDirectQueryDataSources",
        "es:listDomainMaintenances",
        "es:listDomainNames",
        "es:listDomainsForPackage",
        "es:listInstanceTypeDetails",
        "es:listInsights",
        "es:listPackagesForDomain",
        "es:listScheduledActions",
```

```
        "es:listTags",
        "es:listVersions",
        "es:listVpcEndpointAccess",
        "es:listVpcEndpoints",
        "es:listVpcEndpointsForDomain",
        "events:describeApiDestination",
        "events:describeArchive",
        "events:describeConnection",
        "events:describeEndpoint",
        "events:describeEventBus",
        "events:describeEventSource",
        "events:describePartnerEventSource",
        "events:describeReplay",
        "events:describeRule",
        "events:listApiDestinations",
        "events:listArchives",
        "events:listConnections",
        "events:listEndpoints",
        "events:listEventBuses",
        "events:listEventSources",
        "events:listPartnerEventSourceAccounts",
        "events:listPartnerEventSources",
        "events:listReplays",
        "events:listRuleNamesByTarget",
        "events:listRules",
        "events:listTargetsByRule",
        "events:testEventPattern",
        "evs:getEnvironment",
        "evs:getVersions",
        "evs:listEnvironmentHosts",
        "evs:listEnvironments",
        "evs:listEnvironmentVlans",
        "evs:listTagsForResource",
        "firehose:describeDeliveryStream",
        "firehose:listDeliveryStreams",
        "fis:getAction",
        "fis:getExperiment",
        "fis:getExperimentTargetAccountConfiguration",
        "fis:getExperimentTemplate",
        "fis:getSafetyLever",
        "fis:getTargetAccountConfiguration",
        "fis:listActions",
        "fis:listExperimentResolvedTargets",
        "fis:listExperimentTargetAccountConfigurations",
```

```
        "fis:listExperiments",
        "fis:listExperimentTemplates",
        "fis:listTargetAccountConfigurations",
        "fms:getAdminAccount",
        "fms:getAdminScope",
        "fms:getAppsList",
        "fms:getComplianceDetail",
        "fms:getNotificationChannel",
        "fms:getProtocolsList",
        "fms:getPolicy",
        "fms:getProtectionStatus",
        "fms:getResourceSet",
        "fms:getThirdPartyFirewallAssociationStatus",
        "fms:getViolationDetails",
        "fms:listAdminAccountsForOrganization",
        "fms:listAdminsManagingAccount",
        "fms:listAppsLists",
        "fms:listComplianceStatus",
        "fms:listDiscoveredResources",
        "fms:listMemberAccounts",
        "fms:listProtocolsLists",
        "fms:listPolicies",
        "fms:listResourceSetResources",
        "fms:listResourceSets",
        "fms:listThirdPartyFirewallFirewallPolicies",
        "forecast:describeDataset",
        "forecast:describeDatasetGroup",
        "forecast:describeDatasetImportJob",
        "forecast:describeForecast",
        "forecast:describeForecastExportJob",
        "forecast:describePredictor",
        "forecast:getAccuracyMetrics",
        "forecast:listDatasetGroups",
        "forecast:listDatasetImportJobs",
        "forecast:listDatasets",
        "forecast:listForecastExportJobs",
        "forecast:listForecasts",
        "forecast:listPredictors",
        "freetier:getFreeTierUsage",
        "fsx:describeBackups",
        "fsx:describeDataRepositoryAssociations",
        "fsx:describeDataRepositoryTasks",
        "fsx:describeFileCaches",
        "fsx:describeFileSystems",
```

```
        "fsx:describeS3AccessPointAttachments",
        "fsx:describeSnapshots",
        "fsx:describeStorageVirtualMachines",
        "fsx:describeVolumes",
        "fsx:listTagsForResource",
        "gamelift:describeAlias",
        "gamelift:describeBuild",
        "gamelift:describeEC2InstanceLimits",
        "gamelift:describeFleetAttributes",
        "gamelift:describeFleetCapacity",
        "gamelift:describeFleetEvents",
        "gamelift:describeFleetLocationAttributes",
        "gamelift:describeFleetLocationCapacity",
        "gamelift:describeFleetLocationUtilization",
        "gamelift:describeFleetPortSettings",
        "gamelift:describeFleetUtilization",
        "gamelift:describeGameServer",
        "gamelift:describeGameServerGroup",
        "gamelift:describeGameSessionDetails",
        "gamelift:describeGameSessionPlacement",
        "gamelift:describeGameSessionQueues",
        "gamelift:describeGameSessions",
        "gamelift:describeInstances",
        "gamelift:describeMatchmaking",
        "gamelift:describeMatchmakingConfigurations",
        "gamelift:describeMatchmakingRuleSets",
        "gamelift:describePlayerSessions",
        "gamelift:describeRuntimeConfiguration",
        "gamelift:describeScalingPolicies",
        "gamelift:describeScript",
        "gamelift:listAliases",
        "gamelift:listBuilds",
        "gamelift:listFleets",
        "gamelift:listGameServerGroups",
        "gamelift:listGameServers",
        "gamelift:listScripts",
        "gamelift:resolveAlias",
        "geo:calculateRoute",
        "geo:calculateRouteMatrix",
        "geo:describeMap",
        "geo:describePlaceIndex",
        "geo:describeRouteCalculator",
        "geo:describeTracker",
        "geo:getMapGlyphs",
```

```
        "geo:getMapSprites",
        "geo:getMapStyleDescriptor",
        "geo:getMapTile",
        "geo:getPlace",
        "geo:listGeofenceCollections",
        "geo:listMaps",
        "geo:listPlaceIndexes",
        "geo:listRouteCalculators",
        "geo:listTrackerConsumers",
        "geo:searchPlaceIndexForPosition",
        "geo:searchPlaceIndexForSuggestions",
        "geo:searchPlaceIndexForText",
        "geo-maps:getStaticMap",
        "geo-maps:getTile",
        "geo-places:autocomplete",
        "geo-places:geocode",
        "geo-places:getPlace",
        "geo-places:reverseGeocode",
        "geo-places:searchNearby",
        "geo-places:searchText",
        "geo-places:suggest",
        "geo-routes:calculateIsolines",
        "geo-routes:calculateRouteMatrix",
        "geo-routes:calculateRoutes",
        "geo-routes:optimizeWaypoints",
        "geo-routes:snapToRoads",
        "glacier:describeJob",
        "glacier:describeVault",
        "glacier:getDataRetrievalPolicy",
        "glacier:getVaultAccessPolicy",
        "glacier:getVaultLock",
        "glacier:getVaultNotifications",
        "glacier:listJobs",
        "glacier:listTagsForVault",
        "glacier:listVaults",
        "globalaccelerator:describeAccelerator",
        "globalaccelerator:describeAcceleratorAttributes",
        "globalaccelerator:describeCrossAccountAttachment",
        "globalaccelerator:describeCustomRoutingAccelerator",
        "globalaccelerator:describeCustomRoutingAcceleratorAttributes",
        "globalaccelerator:describeCustomRoutingEndpointGroup",
        "globalaccelerator:describeCustomRoutingListener",
        "globalaccelerator:describeEndpointGroup",
        "globalaccelerator:describeListener",
```

```
        "globalaccelerator:listAccelerators",
        "globalaccelerator:listByoipCidrs",
        "globalaccelerator:listCrossAccountAttachments",
        "globalaccelerator:listCrossAccountResourceAccounts",
        "globalaccelerator:listCrossAccountResources",
        "globalaccelerator:listCustomRoutingAccelerators",
        "globalaccelerator:listCustomRoutingEndpointGroups",
        "globalaccelerator:listCustomRoutingListeners",
        "globalaccelerator:listCustomRoutingPortMappings",
        "globalaccelerator:listCustomRoutingPortMappingsByDestination",
        "globalaccelerator:listEndpointGroups",
        "globalaccelerator:listListeners",
        "glue:batchGetBlueprints",
        "glue:batchGetCrawlers",
        "glue:batchGetDevEndpoints",
        "glue:batchGetJobs",
        "glue:batchGetPartition",
        "glue:batchGetTriggers",
        "glue:batchGetWorkflows",
        "glue:checkSchemaVersionValidity",
        "glue:batchGetTableOptimizer",
        "glue:getBlueprint",
        "glue:getBlueprintRun",
        "glue:getBlueprintRuns",
        "glue:getCatalog",
        "glue:getCatalogImportStatus",
        "glue:getCatalogs",
        "glue:getClassifier",
        "glue:getClassifiers",
        "glue:getColumnStatisticsForPartition",
        "glue:getColumnStatisticsForTable",
        "glue:getColumnStatisticsTaskRun",
        "glue:getColumnStatisticsTaskRuns",
        "glue:getCompletion",
        "glue:getCrawler",
        "glue:getCrawlerMetrics",
        "glue:getCrawlers",
        "glue:getCustomEntityType",
        "glue:getDatabase",
        "glue:getDatabases",
        "glue:getDataCatalogEncryptionSettings",
        "glue:getDataflowGraph",
        "glue:getDataQualityResult",
        "glue:getDataQualityRuleRecommendationRun",
```

```
        "glue:getDataQualityRuleset",
        "glue:getDataQualityRulesetEvaluationRun",
        "glue:getDevEndpoint",
        "glue:getDevEndpoints",
        "glue:getJob",
        "glue:getJobBookmark",
        "glue:getJobRun",
        "glue:getJobRuns",
        "glue:getJobs",
        "glue:getMapping",
        "glue:getMLTaskRun",
        "glue:getMLTaskRuns",
        "glue:getMLTransform",
        "glue:getMLTransforms",
        "glue:getPartition",
        "glue:getPartitionIndexes",
        "glue:getPartitions",
        "glue:getRegistry",
        "glue:getResourcePolicies",
        "glue:getResourcePolicy",
        "glue:getSchema",
        "glue:getSchemaByDefinition",
        "glue:getSchemaVersion",
        "glue:getSchemaVersionsDiff",
        "glue:getSecurityConfiguration",
        "glue:getSecurityConfigurations",
        "glue:getSession",
        "glue:getStatement",
        "glue:getTable",
        "glue:getTableOptimizer",
        "glue:getTableVersion",
        "glue:getTables",
        "glue:getTableVersions",
        "glue:getTrigger",
        "glue:getTriggers",
        "glue:getUserDefinedFunction",
        "glue:getUserDefinedFunctions",
        "glue:getWorkflow",
        "glue:getWorkflowRun",
        "glue:getWorkflowRuns",
        "glue:listColumnStatisticsTaskRuns",
        "glue:listCrawlers",
        "glue:listCrawls",
        "glue:listDataQualityResults",
```

```
        "glue:listDataQualityRuleRecommendationRuns",
        "glue:listDataQualityRulesetEvaluationRuns",
        "glue:listDataQualityRulesets",
        "glue:listDevEndpoints",
        "glue:listMLTransforms",
        "glue:listRegistries",
        "glue:listSchemas",
        "glue:listSchemaVersions",
        "glue:listSessions",
        "glue:listStatements",
        "glue:listTableOptimizerRuns",
        "glue:listTriggers",
        "glue:querySchemaVersionMetadata",
        "glue:startCompletion",
        "grafana:describeWorkspace",
        "grafana:describeWorkspaceAuthentication",
        "grafana:listPermissions",
        "grafana:listVersions",
        "grafana:listWorkspaces",
        "greengrass:describeComponent",
        "greengrass:getComponent",
        "greengrass:getConnectivityInfo",
        "greengrass:getCoreDefinition",
        "greengrass:getCoreDefinitionVersion",
        "greengrass:getCoreDevice",
        "greengrass:getDeployment",
        "greengrass:getDeploymentStatus",
        "greengrass:getDeviceDefinition",
        "greengrass:getDeviceDefinitionVersion",
        "greengrass:getFunctionDefinition",
        "greengrass:getFunctionDefinitionVersion",
        "greengrass:getGroup",
        "greengrass:getGroupCertificateAuthority",
        "greengrass:getGroupVersion",
        "greengrass:getLoggerDefinition",
        "greengrass:getLoggerDefinitionVersion",
        "greengrass:getResourceDefinitionVersion",
        "greengrass:getServiceRoleForAccount",
        "greengrass:getSubscriptionDefinition",
        "greengrass:getSubscriptionDefinitionVersion",
        "greengrass:listClientDevicesAssociatedWithCoreDevice",
        "greengrass:listComponents",
        "greengrass:listComponentVersions",
        "greengrass:listCoreDefinitions",
```

```
        "greengrass:listCoreDefinitionVersions",
        "greengrass:listCoreDevices",
        "greengrass:listDeployments",
        "greengrass:listEffectiveDeployments",
        "greengrass:listInstalledComponents",
        "greengrass:listDeviceDefinitions",
        "greengrass:listDeviceDefinitionVersions",
        "greengrass:listFunctionDefinitions",
        "greengrass:listFunctionDefinitionVersions",
        "greengrass:listGroups",
        "greengrass:listGroupVersions",
        "greengrass:listLoggerDefinitions",
        "greengrass:listLoggerDefinitionVersions",
        "greengrass:listResourceDefinitions",
        "greengrass:listResourceDefinitionVersions",
        "greengrass:listSubscriptionDefinitions",
        "greengrass:listSubscriptionDefinitionVersions",
        "guardduty:describeMalwareScans",
        "guardduty:describePublishingDestination",
        "guardduty:getCoverageStatistics",
        "guardduty:getDetector",
        "guardduty:getFilter",
        "guardduty:getFindings",
        "guardduty:getFindingsStatistics",
        "guardduty:getInvitationsCount",
        "guardduty:getIPSet",
        "guardduty:getMalwareProtectionPlan",
        "guardduty:getMalwareScan",
        "guardduty:getMalwareScanSettings",
        "guardduty:getMasterAccount",
        "guardduty:getMemberDetectors",
        "guardduty:getMembers",
        "guardduty:getOrganizationStatistics",
        "guardduty:getRemainingFreeTrialDays",
        "guardduty:getThreatEntitySet",
        "guardduty:getThreatIntelSet",
        "guardduty:getTrustedEntitySet",
        "guardduty:listCoverage",
        "guardduty:listDetectors",
        "guardduty:listFilters",
        "guardduty:listFindings",
        "guardduty:listInvitations",
        "guardduty:listIPSets",
        "guardduty:listMalwareProtectionPlans",
```

```
        "guardduty:listMalwareScans",
        "guardduty:listMembers",
        "guardduty:listThreatIntelSets",
        "health:describeAffectedAccountsForOrganization",
        "health:describeAffectedEntities",
        "health:describeAffectedEntitiesForOrganization",
        "health:describeEntityAggregates",
        "health:describeEntityAggregatesForOrganization",
        "health:describeEventAggregates",
        "health:describeEventDetails",
        "health:describeEventDetailsForOrganization",
        "health:describeEvents",
        "health:describeEventsForOrganization",
        "health:describeEventTypes",
        "health:describeHealthServiceStatusForOrganization",
        "iam:getAccessKeyLastUsed",
        "iam:getAccountAuthorizationDetails",
        "iam:getAccountPasswordPolicy",
        "iam:getAccountSummary",
        "iam:getContextKeysForCustomPolicy",
        "iam:getContextKeysForPrincipalPolicy",
        "iam:getCredentialReport",
        "iam:getGroup",
        "iam:getGroupPolicy",
        "iam:getInstanceProfile",
        "iam:getLoginProfile",
        "iam:getMFADevice",
        "iam:getOpenIDConnectProvider",
        "iam:getPolicy",
        "iam:getPolicyVersion",
        "iam:getRole",
        "iam:getRolePolicy",
        "iam:getSAMLProvider",
        "iam:getServerCertificate",
        "iam:getServiceLinkedRoleDeletionStatus",
        "iam:getSSHPublicKey",
        "iam:getUser",
        "iam:getUserPolicy",
        "iam:listAccessKeys",
        "iam:listAccountAliases",
        "iam:listAttachedGroupPolicies",
        "iam:listAttachedRolePolicies",
        "iam:listAttachedUserPolicies",
        "iam:listEntitiesForPolicy",
```

```
        "iam:listGroupPolicies",
        "iam:listGroups",
        "iam:listGroupsForUser",
        "iam:listInstanceProfiles",
        "iam:listInstanceProfilesForRole",
        "iam:listMFADevices",
        "iam:listOpenIDConnectProviders",
        "iam:listPolicies",
        "iam:listPolicyVersions",
        "iam:listRolePolicies",
        "iam:listRoles",
        "iam:listSAMLProviders",
        "iam:listServerCertificates",
        "iam:listServiceSpecificCredentials",
        "iam:listSigningCertificates",
        "iam:listSSHPublicKeys",
        "iam:listUserPolicies",
        "iam:listUsers",
        "iam:listVirtualMFADevices",
        "iam:simulateCustomPolicy",
        "iam:simulatePrincipalPolicy",
        "identitystore:describeGroup",
        "identitystore:describeGroupMembership",
        "identitystore:describeUser",
        "identitystore:getGroupId",
        "identitystore:getGroupMembershipId",
        "identitystore:getUserId",
        "identitystore:isMemberInGroups",
        "identitystore:listGroupMemberships",
        "identitystore:listGroupMembershipsForMember",
        "identitystore:listGroups",
        "identitystore:listUsers",
        "imagebuilder:getComponent",
        "imagebuilder:getComponentPolicy",
        "imagebuilder:getContainerRecipe",
        "imagebuilder:getContainerRecipePolicy",
        "imagebuilder:getDistributionConfiguration",
        "imagebuilder:getImage",
        "imagebuilder:getImagePipeline",
        "imagebuilder:getImagePolicy",
        "imagebuilder:getImageRecipe",
        "imagebuilder:getImageRecipePolicy",
        "imagebuilder:getInfrastructureConfiguration",
        "imagebuilder:getLifecycleExecution",
```

```
        "imagebuilder:getLifecyclePolicy",
        "imagebuilder:getWorkflow",
        "imagebuilder:getWorkflowExecution",
        "imagebuilder:getWorkflowStepExecution",
        "imagebuilder:listComponentBuildVersions",
        "imagebuilder:listComponents",
        "imagebuilder:listContainerRecipes",
        "imagebuilder:listDistributionConfigurations",
        "imagebuilder:listImageBuildVersions",
        "imagebuilder:listImagePipelineImages",
        "imagebuilder:listImagePipelines",
        "imagebuilder:listImageRecipes",
        "imagebuilder:listImages",
        "imagebuilder:listImageScanFindingAggregations",
        "imagebuilder:listInfrastructureConfigurations",
        "imagebuilder:listLifecycleExecutionResources",
        "imagebuilder:listLifecycleExecutions",
        "imagebuilder:listLifecyclePolicies",
        "imagebuilder:listTagsForResource",
        "imagebuilder:listWorkflowBuildVersions",
        "imagebuilder:listWorkflowExecutions",
        "imagebuilder:listWorkflows",
        "imagebuilder:listWaitingWorkflowSteps",
        "imagebuilder:listWorkflowStepExecutions",
        "inspector-scan:scanSbom",
        "inspector:describeAssessmentRuns",
        "inspector:describeAssessmentTargets",
        "inspector:describeAssessmentTemplates",
        "inspector:describeCrossAccountAccessRole",
        "inspector:describeResourceGroups",
        "inspector:describeRulesPackages",
        "inspector:getTelemetryMetadata",
        "inspector:listAssessmentRunAgents",
        "inspector:listAssessmentRuns",
        "inspector:listAssessmentTargets",
        "inspector:listAssessmentTemplates",
        "inspector:listEventSubscriptions",
        "inspector:listRulesPackages",
        "inspector:listTagsForResource",
        "inspector2:batchGetAccountStatus",
        "inspector2:batchGetFreeTrialInfo",
        "inspector2:describeOrganizationConfiguration",
        "inspector2:getConfiguration",
        "inspector2:getDelegatedAdminAccount",
```

```
        "inspector2:getEc2DeepInspectionConfiguration",
        "inspector2:getMember",
        "inspector2:getSbomExport",
        "inspector2:listCisScanConfigurations",
        "inspector2:listCisScanResultsAggregatedByChecks",
        "inspector2:listCisScanResultsAggregatedByTargetResource",
        "inspector2:listCisScans",
        "inspector2:listCoverage",
        "inspector2:listDelegatedAdminAccounts",
        "inspector2:listFilters",
        "inspector2:listFindings",
        "inspector2:listMembers",
        "inspector2:listUsageTotals",
        "internetmonitor:getHealthEvent",
        "internetmonitor:getMonitor",
        "internetmonitor:listHealthEvents",
        "internetmonitor:listMonitors",
        "invoicing:batchGetInvoiceProfile",
        "invoicing:listInvoiceSummaries",
        "invoicing:listInvoiceUnits",
        "iot:describeAuthorizer",
        "iot:describeCACertificate",
        "iot:describeCertificate",
        "iot:describeDefaultAuthorizer",
        "iot:describeDomainConfiguration",
        "iot:describeEndpoint",
        "iot:describeIndex",
        "iot:describeJobExecution",
        "iot:describeThing",
        "iot:describeThingGroup",
        "iot:describeTunnel",
        "iot:getEffectivePolicies",
        "iot:getIndexingConfiguration",
        "iot:getLoggingOptions",
        "iot:getPolicy",
        "iot:getPolicyVersion",
        "iot:getTopicRule",
        "iot:getV2LoggingOptions",
        "iot:listAttachedPolicies",
        "iot:listAuthorizers",
        "iot:listCACertificates",
        "iot:listCertificates",
        "iot:listCertificatesByCA",
        "iot:listCommandExecutions",
```

```
        "iot:listCommands",
        "iot:listDomainConfigurations",
        "iot:listJobExecutionsForJob",
        "iot:listJobExecutionsForThing",
        "iot:listJobs",
        "iot:listNamedShadowsForThing",
        "iot:listOutgoingCertificates",
        "iot:listPackages",
        "iot:listPackageVersions",
        "iot:listPolicies",
        "iot:listPolicyPrincipals",
        "iot:listPolicyVersions",
        "iot:listPrincipalPolicies",
        "iot:listPrincipalThings",
        "iot:listRoleAliases",
        "iot:listTargetsForPolicy",
        "iot:listThingGroups",
        "iot:listThingGroupsForThing",
        "iot:listThingPrincipals",
        "iot:listThingRegistrationTasks",
        "iot:listThings",
        "iot:listThingsInThingGroup",
        "iot:listThingTypes",
        "iot:listTopicRules",
        "iot:listTunnels",
        "iot:listV2LoggingLevels",
        "iotevents:describeDetector",
        "iotevents:describeDetectorModel",
        "iotevents:describeInput",
        "iotevents:describeLoggingOptions",
        "iotevents:listDetectorModels",
        "iotevents:listDetectorModelVersions",
        "iotevents:listDetectors",
        "iotevents:listInputs",
        "iotfleetwise:getCampaign",
        "iotfleetwise:getDecoderManifest",
        "iotfleetwise:getEncryptionConfiguration",
        "iotfleetwise:getFleet",
        "iotfleetwise:getLoggingOptions",
        "iotfleetwise:getModelManifest",
        "iotfleetwise:getRegisterAccountStatus",
        "iotfleetwise:getSignalCatalog",
        "iotfleetwise:getStateTemplate",
        "iotfleetwise:getVehicle",
```

```
        "iotfleetwise:getVehicleStatus",
        "iotfleetwise:listCampaigns",
        "iotfleetwise:listDecoderManifestNetworkInterfaces",
        "iotfleetwise:listDecoderManifests",
        "iotfleetwise:listDecoderManifestSignals",
        "iotfleetwise:listFleets",
        "iotfleetwise:listFleetsForVehicle",
        "iotfleetwise:listModelManifestNodes",
        "iotfleetwise:listModelManifests",
        "iotfleetwise:listSignalCatalogNodes",
        "iotfleetwise:listSignalCatalogs",
        "iotfleetwise:listStateTemplates",
        "iotfleetwise:listVehicles",
        "iotfleetwise:listVehiclesInFleet",
        "iotsitewise:describeAccessPolicy",
        "iotsitewise:describeAsset",
        "iotsitewise:describeAssetModel",
        "iotsitewise:describeAssetProperty",
        "iotsitewise:describeDashboard",
        "iotsitewise:describeGateway",
        "iotsitewise:describeGatewayCapabilityConfiguration",
        "iotsitewise:describeLoggingOptions",
        "iotsitewise:describePortal",
        "iotsitewise:describeProject",
        "iotsitewise:listAccessPolicies",
        "iotsitewise:listAssetModels",
        "iotsitewise:listAssets",
        "iotsitewise:listAssociatedAssets",
        "iotsitewise:listDashboards",
        "iotsitewise:listGateways",
        "iotsitewise:listPortals",
        "iotsitewise:listProjectAssets",
        "iotsitewise:listProjects",
        "iottwinmaker:getComponentType",
        "iottwinmaker:getEntity",
        "iottwinmaker:getPricingPlan",
        "iottwinmaker:getScene",
        "iottwinmaker:getSyncJob",
        "iottwinmaker:getWorkspace",
        "iottwinmaker:listComponentTypes",
        "iottwinmaker:listEntities",
        "iottwinmaker:listScenes",
        "iottwinmaker:listSyncJobs",
        "iottwinmaker:listSyncResources",
```

```
        "iottwinmaker:listWorkspaces",
        "iotwireless:getDestination",
        "iotwireless:getDeviceProfile",
        "iotwireless:getPartnerAccount",
        "iotwireless:getServiceEndpoint",
        "iotwireless:getServiceProfile",
        "iotwireless:getWirelessDevice",
        "iotwireless:getWirelessDeviceStatistics",
        "iotwireless:getWirelessGateway",
        "iotwireless:getWirelessGatewayCertificate",
        "iotwireless:getWirelessGatewayFirmwareInformation",
        "iotwireless:getWirelessGatewayStatistics",
        "iotwireless:getWirelessGatewayTask",
        "iotwireless:getWirelessGatewayTaskDefinition",
        "iotwireless:listDestinations",
        "iotwireless:listDeviceProfiles",
        "iotwireless:listPartnerAccounts",
        "iotwireless:listServiceProfiles",
        "iotwireless:listTagsForResource",
        "iotwireless:listWirelessDevices",
        "iotwireless:listWirelessGateways",
        "iotwireless:listWirelessGatewayTaskDefinitions",
        "ivs:getChannel",
        "ivs:getRecordingConfiguration",
        "ivs:getStream",
        "ivs:getStreamSession",
        "ivs:listChannels",
        "ivs:listPlaybackKeyPairs",
        "ivs:listRecordingConfigurations",
        "ivs:listStreamKeys",
        "ivs:listStreams",
        "ivs:listStreamSessions",
        "kafka:describeCluster",
        "kafka:describeClusterOperation",
        "kafka:describeClusterOperationV2",
        "kafka:describeClusterV2",
        "kafka:describeConfiguration",
        "kafka:describeConfigurationRevision",
        "kafka:describeReplicator",
        "kafka:describeTopic",
        "kafka:describeTopicPartitions",
        "kafka:describeVpcConnection",
        "kafka:getBootstrapBrokers",
        "kafka:getClusterPolicy",
```

```
        "kafka:getCompatibleKafkaVersions",
        "kafka:listClientVpcConnections",
        "kafka:listClusterOperations",
        "kafka:listClusterOperationsV2",
        "kafka:listClusters",
        "kafka:listClustersV2",
        "kafka:listConfigurationRevisions",
        "kafka:listConfigurations",
        "kafka:listNodes",
        "kafka:listReplicators",
        "kafka:listScramSecrets",
        "kafka:listTagsForResource",
        "kafka:listTopics",
        "kafka:listVpcConnections",
        "kafkaconnect:describeConnector",
        "kafkaconnect:describeCustomPlugin",
        "kafkaconnect:describeWorkerConfiguration",
        "kafkaconnect:listConnectors",
        "kafkaconnect:listCustomPlugins",
        "kafkaconnect:listWorkerConfigurations",
        "kendra:describeAccessControlConfiguration",
        "kendra:describeDataSource",
        "kendra:describeExperience",
        "kendra:describeFaq",
        "kendra:describeFeaturedResultsSet",
        "kendra:describeIndex",
        "kendra:describePrincipalMapping",
        "kendra:describeQuerySuggestionsBlockList",
        "kendra:describeQuerySuggestionsConfig",
        "kendra:describeThesaurus",
        "kendra:listAccessControlConfigurations",
        "kendra:listDataSourceSyncJobs",
        "kendra:listDataSources",
        "kendra:listEntityPersonas",
        "kendra:listExperienceEntities",
        "kendra:listExperiences",
        "kendra:listFaqs",
        "kendra:listFeaturedResultsSets",
        "kendra:listIndices",
        "kendra:listQuerySuggestionsBlockLists",
        "kendra:listThesauri",
        "kinesis:describeStream",
        "kinesis:describeStreamConsumer",
        "kinesis:describeStreamSummary",
```

```
        "kinesis:listShards",
        "kinesis:listStreamConsumers",
        "kinesis:listStreams",
        "kinesis:listTagsForStream",
        "kinesisanalytics:describeApplication",
        "kinesisanalytics:describeApplicationOperation",
        "kinesisanalytics:describeApplicationSnapshot",
        "kinesisanalytics:listApplicationOperations",
        "kinesisanalytics:listApplications",
        "kinesisanalytics:listApplicationSnapshots",
        "kinesisanalytics:listApplicationVersions",
        "kinesisvideo:describeImageGenerationConfiguration",
        "kinesisvideo:describeEdgeConfiguration",
        "kinesisvideo:describeMappedResourceConfiguration",
        "kinesisvideo:describeMediaStorageConfiguration",
        "kinesisvideo:describeNotificationConfiguration",
        "kinesisvideo:describeSignalingChannel",
        "kinesisvideo:describeStream",
        "kinesisvideo:getDataEndpoint",
        "kinesisvideo:getIceServerConfig",
        "kinesisvideo:getSignalingChannelEndpoint",
        "kinesisvideo:listSignalingChannels",
        "kinesisvideo:listEdgeAgentConfigurations",
        "kinesisvideo:listStreams",
        "kms:describeCustomKeyStores",
        "kms:describeKey",
        "kms:getKeyPolicy",
        "kms:getKeyRotationStatus",
        "kms:listAliases",
        "kms:listGrants",
        "kms:listKeyPolicies",
        "kms:listKeyRotations",
        "kms:listKeys",
        "kms:listResourceTags",
        "kms:listRetirableGrants",
        "lakeformation:describeLakeFormationIdentityCenterConfiguration",
        "lakeformation:describeResource",
        "lakeformation:describeTransaction",
        "lakeformation:getDataLakePrincipal",
        "lakeformation:getDataLakeSettings",
        "lakeformation:getEffectivePermissionsForPath",
        "lakeformation:getLFTag",
        "lakeformation:getLFTagExpression",
        "lakeformation:getQueryState",
```

```
        "lakeformation:getQueryStatistics",
        "lakeformation:getResourceLFTags",
        "lakeformation:listLFTagExpressions",
        "lakeformation:listLFTags",
        "lakeformation:listLakeFormationOptIns",
        "lakeformation:listPermissions",
        "lakeformation:listResources",
        "lakeformation:searchDatabasesByLFTags",
        "lakeformation:searchTablesByLFTags",
        "lambda:getAccountSettings",
        "lambda:getAlias",
        "lambda:getCodeSigningConfig",
        "lambda:getDurableExecution",
        "lambda:getDurableExecutionHistory",
        "lambda:getDurableExecutionState",
        "lambda:getEventSourceMapping",
        "lambda:getFunction",
        "lambda:getFunctionCodeSigningConfig",
        "lambda:getFunctionConcurrency",
        "lambda:getFunctionConfiguration",
        "lambda:getFunctionEventInvokeConfig",
        "lambda:getFunctionRecursionConfig",
        "lambda:getFunctionScalingConfig",
        "lambda:getFunctionUrlConfig",
        "lambda:getLayerVersion",
        "lambda:getLayerVersionPolicy",
        "lambda:getMicrovm",
        "lambda:getMicrovmImage",
        "lambda:getMicrovmImageBuild",
        "lambda:getMicrovmImageVersion",
        "lambda:getPolicy",
        "lambda:getCapacityProvider",
        "lambda:getProvisionedConcurrencyConfig",
        "lambda:getRuntimeManagementConfig",
        "lambda:listAliases",
        "lambda:listCapacityProviders",
        "lambda:listCodeSigningConfigs",
        "lambda:listDurableExecutionsByFunction",
        "lambda:listEventSourceMappings",
        "lambda:listFunctionEventInvokeConfigs",
        "lambda:listFunctions",
        "lambda:listFunctionsByCodeSigningConfig",
        "lambda:listFunctionUrlConfigs",
        "lambda:listFunctionVersionsByCapacityProvider",
```

```
        "lambda:listLayers",
        "lambda:listLayerVersions",
        "lambda:listManagedMicrovmImages",
        "lambda:listManagedMicrovmImageVersions",
        "lambda:listMicrovmImageBuilds",
        "lambda:listMicrovmImages",
        "lambda:listMicrovmImageVersions",
        "lambda:listMicrovms",
        "lambda:listProvisionedConcurrencyConfigs",
        "lambda:listTags",
        "lambda:listVersionsByFunction",
        "launchwizard:describeProvisionedApp",
        "launchwizard:describeProvisioningEvents",
        "launchwizard:listDeploymentEvents",
        "launchwizard:listDeployments",
        "launchwizard:listProvisionedApps",
        "lex:describeBot",
        "lex:describeBotAlias",
        "lex:describeBotLocale",
        "lex:describeBotRecommendation",
        "lex:describeBotVersion",
        "lex:describeCustomVocabularyMetadata",
        "lex:describeExport",
        "lex:describeImport",
        "lex:describeIntent",
        "lex:describeResourcePolicy",
        "lex:describeSlot",
        "lex:describeSlotType",
        "lex:getBot",
        "lex:getBotAlias",
        "lex:getBotAliases",
        "lex:getBotChannelAssociation",
        "lex:getBotChannelAssociations",
        "lex:getBots",
        "lex:getBotVersions",
        "lex:getBuiltinIntent",
        "lex:getBuiltinIntents",
        "lex:getBuiltinSlotTypes",
        "lex:getIntent",
        "lex:getIntents",
        "lex:getIntentVersions",
        "lex:getSlotType",
        "lex:getSlotTypes",
        "lex:getSlotTypeVersions",
```

```
        "lex:listBotAliases",
        "lex:listBotLocales",
        "lex:listBotRecommendations",
        "lex:listBots",
        "lex:listBotVersions",
        "lex:listExports",
        "lex:listImports",
        "lex:listIntents",
        "lex:listRecommendedIntents",
        "lex:listSlots",
        "lex:listSlotTypes",
        "license-manager:getGrant",
        "license-manager:getLicense",
        "license-manager:getLicenseConfiguration",
        "license-manager:getLicenseConversionTask",
        "license-manager:getLicenseManagerReportGenerator",
        "license-manager:getLicenseUsage",
        "license-manager:getServiceSettings",
        "license-manager:listAssociationsForLicenseConfiguration",
        "license-manager:listDistributedGrants",
        "license-manager:listFailuresForLicenseConfigurationOperations",
        "license-manager:listLicenseConfigurations",
        "license-manager:listLicenseConversionTasks",
        "license-manager:listLicenseManagerReportGenerators",
        "license-manager:listLicenses",
        "license-manager:listLicenseSpecificationsForResource",
        "license-manager:listLicenseVersions",
        "license-manager:listReceivedGrants",
        "license-manager:listReceivedGrantsForOrganization",
        "license-manager:listReceivedLicenses",
        "license-manager:listReceivedLicensesForOrganization",
        "license-manager:listResourceInventory",
        "license-manager:listTokens",
        "license-manager:listUsageForLicenseConfiguration",
        "license-manager-linux-subscriptions:getRegisteredSubscriptionProvider",
        "license-manager-linux-subscriptions:getServiceSettings",
        "license-manager-linux-subscriptions:listLinuxSubscriptionInstances",
        "license-manager-linux-subscriptions:listLinuxSubscriptions",
        "license-manager-linux-subscriptions:listRegisteredSubscriptionProviders",
        "license-manager-user-subscriptions:listIdentityProviders",
        "license-manager-user-subscriptions:listInstances",
        "license-manager-user-subscriptions:listLicenseServerEndpoints",
        "license-manager-user-subscriptions:listProductSubscriptions",
        "license-manager-user-subscriptions:listUserAssociations",
```

```
        "lightsail:getActiveNames",
        "lightsail:getAlarms",
        "lightsail:getAutoSnapshots",
        "lightsail:getBlueprints",
        "lightsail:getBucketBundles",
        "lightsail:getBucketMetricData",
        "lightsail:getBuckets",
        "lightsail:getBundles",
        "lightsail:getCertificates",
        "lightsail:getContainerImages",
        "lightsail:getContainerServiceDeployments",
        "lightsail:getContainerServiceMetricData",
        "lightsail:getContainerServicePowers",
        "lightsail:getContainerServices",
        "lightsail:getDisk",
        "lightsail:getDisks",
        "lightsail:getDiskSnapshot",
        "lightsail:getDiskSnapshots",
        "lightsail:getDistributionBundles",
        "lightsail:getDistributionMetricData",
        "lightsail:getDistributions",
        "lightsail:getDomain",
        "lightsail:getDomains",
        "lightsail:getExportSnapshotRecords",
        "lightsail:getInstance",
        "lightsail:getInstanceMetricData",
        "lightsail:getInstancePortStates",
        "lightsail:getInstances",
        "lightsail:getInstanceSnapshot",
        "lightsail:getInstanceSnapshots",
        "lightsail:getInstanceState",
        "lightsail:getKeyPair",
        "lightsail:getKeyPairs",
        "lightsail:getLoadBalancer",
        "lightsail:getLoadBalancerMetricData",
        "lightsail:getLoadBalancers",
        "lightsail:getLoadBalancerTlsCertificates",
        "lightsail:getOperation",
        "lightsail:getOperations",
        "lightsail:getOperationsForResource",
        "lightsail:getRegions",
        "lightsail:getRelationalDatabase",
        "lightsail:getRelationalDatabaseMetricData",
        "lightsail:getRelationalDatabases",
```

```
        "lightsail:getRelationalDatabaseSnapshot",
        "lightsail:getRelationalDatabaseSnapshots",
        "lightsail:getStaticIp",
        "lightsail:getStaticIps",
        "lightsail:isVpcPeered",
        "logs:describeAccountPolicies",
        "logs:describeDeliveries",
        "logs:describeDeliveryDestinations",
        "logs:describeDeliverySources",
        "logs:describeDestinations",
        "logs:describeExportTasks",
        "logs:describeFieldIndexes",
        "logs:describeIndexPolicies",
        "logs:describeLogGroups",
        "logs:describeLogStreams",
        "logs:describeMetricFilters",
        "logs:describeQueries",
        "logs:describeQueryDefinitions",
        "logs:describeResourcePolicies",
        "logs:describeSubscriptionFilters",
        "logs:getDataProtectionPolicy",
        "logs:getDelivery",
        "logs:getDeliveryDestination",
        "logs:getDeliveryDestinationPolicy",
        "logs:getDeliverySource",
        "logs:getIntegration",
        "logs:getLogAnomalyDetector",
        "logs:getLogDelivery",
        "logs:getLogGroupFields",
        "logs:getTransformer",
        "logs:listAnomalies",
        "logs:listIntegrations",
        "logs:listLogAnomalyDetectors",
        "logs:listLogDeliveries",
        "logs:listLogGroups",
        "logs:listLogGroupsForQuery",
        "logs:testMetricFilter",
        "lookoutequipment:describeDataIngestionJob",
        "lookoutequipment:describeDataset",
        "lookoutequipment:describeInferenceScheduler",
        "lookoutequipment:describeModel",
        "lookoutequipment:listDataIngestionJobs",
        "lookoutequipment:listDatasets",
        "lookoutequipment:listInferenceExecutions",
```

```
        "lookoutequipment:listInferenceSchedulers",
        "lookoutequipment:listModels",
        "m2:getApplication",
        "m2:getApplicationVersion",
        "m2:getBatchJobExecution",
        "m2:getDataSetDetails",
        "m2:getDataSetImportTask",
        "m2:getDeployment",
        "m2:getEnvironment",
        "m2:listApplications",
        "m2:listApplicationVersions",
        "m2:listBatchJobDefinitions",
        "m2:listBatchJobExecutions",
        "m2:listDataSetImportHistory",
        "m2:listDataSets",
        "m2:listDeployments",
        "m2:listEngineVersions",
        "m2:listEnvironments",
        "machinelearning:describeBatchPredictions",
        "machinelearning:describeDataSources",
        "machinelearning:describeEvaluations",
        "machinelearning:describeMLModels",
        "machinelearning:getBatchPrediction",
        "machinelearning:getDataSource",
        "machinelearning:getEvaluation",
        "machinelearning:getMLModel",
        "macie2:describeBuckets",
        "macie2:describeClassificationJob",
        "macie2:getAdministratorAccount",
        "macie2:getAllowList",
        "macie2:getAutomatedDiscoveryConfiguration",
        "macie2:getClassificationExportConfiguration",
        "macie2:getClassificationScope",
        "macie2:getCustomDataIdentifier",
        "macie2:getFindings",
        "macie2:getFindingsFilter",
        "macie2:getFindingsPublicationConfiguration",
        "macie2:getFindingStatistics",
        "macie2:getMacieSession",
        "macie2:getMember",
        "macie2:getResourceProfile",
        "macie2:getRevealConfiguration",
        "macie2:getSensitivityInspectionTemplate",
        "macie2:getUsageStatistics",
```

```
        "macie2:listAllowLists",
        "macie2:listAutomatedDiscoveryAccounts",
        "macie2:listClassificationJobs",
        "macie2:listClassificationScopes",
        "macie2:listCustomDataIdentifiers",
        "macie2:listFindings",
        "macie2:listFindingsFilters",
        "macie2:listMembers",
        "macie2:listSensitivityInspectionTemplates",
        "managedblockchain:getMember",
        "managedblockchain:getNetwork",
        "managedblockchain:getNode",
        "managedblockchain:listMembers",
        "managedblockchain:listNetworks",
        "managedblockchain:listNodes",
        "mediaconnect:describeFlow",
        "mediaconnect:listEntitlements",
        "mediaconnect:listFlows",
        "mediaconvert:describeEndpoints",
        "mediaconvert:getJob",
        "mediaconvert:getJobTemplate",
        "mediaconvert:getPreset",
        "mediaconvert:getQueue",
        "mediaconvert:listJobs",
        "mediaconvert:listJobTemplates",
        "medialive:describeChannel",
        "medialive:describeInput",
        "medialive:describeInputDevice",
        "medialive:describeInputSecurityGroup",
        "medialive:describeMultiplex",
        "medialive:describeOffering",
        "medialive:describeReservation",
        "medialive:describeSchedule",
        "medialive:getCloudWatchAlarmTemplate",
        "medialive:getCloudWatchAlarmTemplateGroup",
        "medialive:getEventBridgeRuleTemplate",
        "medialive:getEventBridgeRuleTemplateGroup",
        "medialive:getSignalMap",
        "medialive:listChannels",
        "medialive:listCloudWatchAlarmTemplateGroups",
        "medialive:listCloudWatchAlarmTemplates",
        "medialive:listEventBridgeRuleTemplateGroups",
        "medialive:listEventBridgeRuleTemplates",
        "medialive:listInputDevices",
```

```
        "medialive:listInputs",
        "medialive:listInputSecurityGroups",
        "medialive:listMultiplexes",
        "medialive:listOfferings",
        "medialive:listReservations",
        "medialive:listSignalMaps",
        "mediapackage:describeChannel",
        "mediapackage:describeOriginEndpoint",
        "mediapackage:listChannels",
        "mediapackage:listOriginEndpoints",
        "mediastore:describeContainer",
        "mediastore:getContainerPolicy",
        "mediastore:getCorsPolicy",
        "mediastore:listContainers",
        "mediatailor:getPlaybackConfiguration",
        "mediatailor:listPlaybackConfigurations",
        "medical-imaging:getDatastore",
        "medical-imaging:listDatastores",
        "memorydb:describeReservedNodesOfferings",
        "memorydb:listAllowedNodeTypeUpdates",
        "mgn:describeJobLogItems",
        "mgn:describeJobs",
        "mgn:describeLaunchConfigurationTemplates",
        "mgn:describeReplicationConfigurationTemplates",
        "mgn:describeSourceServers",
        "mgn:describeVcenterClients",
        "mgn:getLaunchConfiguration",
        "mgn:getReplicationConfiguration",
        "mgn:listApplications",
        "mgn:listSourceServerActions",
        "mgn:listTemplateActions",
        "mgn:listWaves",
        "mobiletargeting:getAdmChannel",
        "mobiletargeting:getApnsChannel",
        "mobiletargeting:getApnsSandboxChannel",
        "mobiletargeting:getApnsVoipChannel",
        "mobiletargeting:getApnsVoipSandboxChannel",
        "mobiletargeting:getApp",
        "mobiletargeting:getApplicationSettings",
        "mobiletargeting:getApps",
        "mobiletargeting:getBaiduChannel",
        "mobiletargeting:getCampaign",
        "mobiletargeting:getCampaignActivities",
        "mobiletargeting:getCampaigns",
```

```
        "mobiletargeting:getCampaignVersion",
        "mobiletargeting:getCampaignVersions",
        "mobiletargeting:getEmailChannel",
        "mobiletargeting:getEndpoint",
        "mobiletargeting:getEventStream",
        "mobiletargeting:getExportJob",
        "mobiletargeting:getExportJobs",
        "mobiletargeting:getGcmChannel",
        "mobiletargeting:getImportJob",
        "mobiletargeting:getImportJobs",
        "mobiletargeting:getJourney",
        "mobiletargeting:getJourneyExecutionActivityMetrics",
        "mobiletargeting:getJourneyExecutionMetrics",
        "mobiletargeting:getJourneyRunExecutionActivityMetrics",
        "mobiletargeting:getJourneyRunExecutionMetrics",
        "mobiletargeting:getJourneyRuns",
        "mobiletargeting:getSegment",
        "mobiletargeting:getSegmentImportJobs",
        "mobiletargeting:getSegments",
        "mobiletargeting:getSegmentVersion",
        "mobiletargeting:getSegmentVersions",
        "mobiletargeting:getSmsChannel",
        "mobiletargeting:listJourneys",
        "mobiletargeting:phoneNumberValidate",
        "mpa:getApprovalTeam",
        "mpa:getSession",
        "mpa:listApprovalTeams",
        "mq:describeBrokerInstanceOptions",
        "mq:describeBroker",
        "mq:describeConfiguration",
        "mq:describeConfigurationRevision",
        "mq:describeUser",
        "mq:listBrokers",
        "mq:listConfigurationRevisions",
        "mq:listConfigurations",
        "mq:listUsers",
        "network-firewall:describeFirewall",
        "network-firewall:describeFirewallPolicy",
        "network-firewall:describeFlowOperation",
        "network-firewall:describeLoggingConfiguration",
        "network-firewall:describeResourcePolicy",
        "network-firewall:describeRuleGroup",
        "network-firewall:describeRuleGroupMetadata",
        "network-firewall:describeTlsInspectionConfiguration",
```

```
        "network-firewall:describeVpcEndpointAssociation",
        "network-firewall:listAnalysisReports",
        "network-firewall:listFirewallPolicies",
        "network-firewall:listFirewalls",
        "network-firewall:listFlowOperationResults",
        "network-firewall:listFlowOperations",
        "network-firewall:listRuleGroups",
        "network-firewall:listTlsInspectionConfigurations",
        "network-firewall:listVpcEndpointAssociations",
        "networkflowmonitor:getMonitor",
        "networkflowmonitor:getScope",
        "networkflowmonitor:listMonitors",
        "networkflowmonitor:listScopes",
        "networkmanager:describeGlobalNetworks",
        "networkmanager:getConnectAttachment",
        "networkmanager:getConnections",
        "networkmanager:getConnectPeer",
        "networkmanager:getConnectPeerAssociations",
        "networkmanager:getCoreNetwork",
        "networkmanager:getCoreNetworkChangeEvents",
        "networkmanager:getCoreNetworkChangeSet",
        "networkmanager:getCoreNetworkPolicy",
        "networkmanager:getCustomerGatewayAssociations",
        "networkmanager:getDevices",
        "networkmanager:getDirectConnectGatewayAttachment",
        "networkmanager:getLinkAssociations",
        "networkmanager:getLinks",
        "networkmanager:getNetworkResourceCounts",
        "networkmanager:getNetworkResourceRelationships",
        "networkmanager:getNetworkResources",
        "networkmanager:getNetworkRoutes",
        "networkmanager:getNetworkTelemetry",
        "networkmanager:getResourcePolicy",
        "networkmanager:getRouteAnalysis",
        "networkmanager:getSites",
        "networkmanager:getSiteToSiteVpnAttachment",
        "networkmanager:getTransitGatewayConnectPeerAssociations",
        "networkmanager:getTransitGatewayPeering",
        "networkmanager:getTransitGatewayRegistrations",
        "networkmanager:getTransitGatewayRouteTableAttachment",
        "networkmanager:getVpcAttachment",
        "networkmanager:listAttachments",
        "networkmanager:listConnectPeers",
        "networkmanager:listCoreNetworkPolicyVersions",
```

```
        "networkmanager:listCoreNetworks",
        "networkmanager:listOrganizationServiceAccessStatus",
        "networkmanager:listPeerings",
        "networkmanager:listTagsForResource",
        "networkmonitor:getMonitor",
        "networkmonitor:getProbe",
        "networkmonitor:listMonitors",
        "notifications-contacts:getEmailContact",
        "notifications-contacts:listEmailContacts",
        "notifications:getEventRule",
        "notifications:getNotificationConfiguration",
        "notifications:getNotificationEvent",
        "notifications:listChannels",
        "notifications:listEventRules",
        "notifications:listNotificationConfigurations",
        "notifications:listNotificationEvents",
        "notifications:listNotificationHubs",
        "oam:getLink",
        "oam:getSink",
        "oam:getSinkPolicy",
        "oam:listAttachedLinks",
        "oam:listLinks",
        "oam:listSinks",
        "observabilityadmin:getTelemetryEvaluationStatus",
        "observabilityadmin:getTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:listResourceTelemetry",
        "observabilityadmin:listResourceTelemetryForOrganization",
        "odb:getCloudAutonomousVmCluster",
        "odb:getCloudExadataInfrastructure",
        "odb:getCloudExadataInfrastructureUnallocatedResources",
        "odb:getCloudVmCluster",
        "odb:getOciOnboardingStatus",
        "odb:getOdbNetwork",
        "odb:getOdbPeeringConnection",
        "odb:listCloudAutonomousVmClusters",
        "odb:listCloudExadataInfrastructures",
        "odb:listCloudVmClusters",
        "odb:listOdbNetworks",
        "odb:listOdbPeeringConnections",
        "omics:getAnnotationImportJob",
        "omics:getAnnotationStore",
        "omics:getAnnotationStoreVersion",
        "omics:getReadSetActivationJob",
        "omics:getReadSetExportJob",
```

```
        "omics:getReadSetImportJob",
        "omics:getReadSetMetadata",
        "omics:getReference",
        "omics:getReferenceImportJob",
        "omics:getReferenceMetadata",
        "omics:getReferenceStore",
        "omics:getRun",
        "omics:getRunCache",
        "omics:getRunGroup",
        "omics:getRunTask",
        "omics:getSequenceStore",
        "omics:getShare",
        "omics:getVariantImportJob",
        "omics:getVariantStore",
        "omics:getWorkflow",
        "omics:getWorkflowVersion",
        "omics:listAnnotationImportJobs",
        "omics:listAnnotationStores",
        "omics:listAnnotationStoreVersions",
        "omics:listMultipartReadSetUploads",
        "omics:listReadSetActivationJobs",
        "omics:listReadSetExportJobs",
        "omics:listReadSetImportJobs",
        "omics:listReadSets",
        "omics:listReadSetUploadParts",
        "omics:listReferenceImportJobs",
        "omics:listReferences",
        "omics:listReferenceStores",
        "omics:listRunCaches"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSSupportActionsGroup3",
      "Effect" : "Allow",
      "Action" : [
        "omics:listRunGroups",
        "omics:listRuns",
        "omics:listRunTasks",
        "omics:listSequenceStores",
        "omics:listShares",
        "omics:listVariantImportJobs",
```

```
        "omics:listVariantStores",
        "omics:listWorkflows",
        "omics:listWorkflowVersions",
        "opsworks-cm:describeAccountAttributes",
        "opsworks-cm:describeBackups",
        "opsworks-cm:describeEvents",
        "opsworks-cm:describeNodeAssociationStatus",
        "opsworks-cm:describeServers",
        "opsworks:describeAgentVersions",
        "opsworks:describeApps",
        "opsworks:describeCommands",
        "opsworks:describeDeployments",
        "opsworks:describeEcsClusters",
        "opsworks:describeElasticIps",
        "opsworks:describeElasticLoadBalancers",
        "opsworks:describeInstances",
        "opsworks:describeLayers",
        "opsworks:describeLoadBasedAutoScaling",
        "opsworks:describeMyUserProfile",
        "opsworks:describePermissions",
        "opsworks:describeRaidArrays",
        "opsworks:describeRdsDbInstances",
        "opsworks:describeServiceErrors",
        "opsworks:describeStackProvisioningParameters",
        "opsworks:describeStacks",
        "opsworks:describeStackSummary",
        "opsworks:describeTimeBasedAutoScaling",
        "opsworks:describeUserProfiles",
        "opsworks:describeVolumes",
        "opsworks:getHostnameSuggestion",
        "organizations:describeAccount",
        "organizations:describeCreateAccountStatus",
        "organizations:describeEffectivePolicy",
        "organizations:describeHandshake",
        "organizations:describeOrganization",
        "organizations:describeOrganizationalUnit",
        "organizations:describePolicy",
        "organizations:describeResourcePolicy",
        "organizations:listAccounts",
        "organizations:listAccountsForParent",
        "organizations:listAWSServiceAccessForOrganization",
        "organizations:listChildren",
        "organizations:listCreateAccountStatus",
        "organizations:listDelegatedAdministrators",
```

```
        "organizations:listDelegatedServicesForAccount",
        "organizations:listHandshakesForAccount",
        "organizations:listHandshakesForOrganization",
        "organizations:listOrganizationalUnitsForParent",
        "organizations:listParents",
        "organizations:listPolicies",
        "organizations:listPoliciesForTarget",
        "organizations:listRoots",
        "organizations:listTagsForResource",
        "organizations:listTargetsForPolicy",
        "osis:getPipeline",
        "osis:getPipelineBlueprint",
        "osis:getPipelineChangeProgress",
        "osis:listPipelineBlueprints",
        "osis:listPipelines",
        "osis:validatePipeline",
        "outposts:getCapacityTask",
        "outposts:getCatalogItem",
        "outposts:getConnection",
        "outposts:getOrder",
        "outposts:getOutpost",
        "outposts:getOutpostInstanceTypes",
        "outposts:getOutpostSupportedInstanceTypes",
        "outposts:getSite",
        "outposts:listAssets",
        "outposts:listAssetInstances",
        "outposts:listBlockingInstancesForCapacityTask",
        "outposts:listCapacityTasks",
        "outposts:listCatalogItems",
        "outposts:listOrders",
        "outposts:listOutposts",
        "outposts:listSites",
        "payment-cryptography:getAlias",
        "payment-cryptography:getKey",
        "payment-cryptography:listAliases",
        "payment-cryptography:listKeys",
        "pca-connector-ad:listConnectors",
        "pca-connector-ad:listDirectoryRegistrations",
        "pca-connector-ad:listServicePrincipalNames",
        "pca-connector-ad:listTagsForResource",
        "pca-connector-ad:listTemplateGroupAccessControlEntries",
        "pca-connector-ad:listTemplates",
        "pcs:getCluster",
        "pcs:getComputeNodeGroup",
```

```
        "pcs:getQueue",
        "pcs:listClusters",
        "pcs:listComputeNodeGroups",
        "pcs:listQueues",
        "personalize:describeAlgorithm",
        "personalize:describeBatchInferenceJob",
        "personalize:describeBatchSegmentJob",
        "personalize:describeCampaign",
        "personalize:describeDataInsightsJob",
        "personalize:describeDataset",
        "personalize:describeDatasetExportJob",
        "personalize:describeDatasetGroup",
        "personalize:describeDatasetImportJob",
        "personalize:describeEventTracker",
        "personalize:describeFeatureTransformation",
        "personalize:describeFilter",
        "personalize:describeMetricAttribution",
        "personalize:describeRecipe",
        "personalize:describeRecommender",
        "personalize:describeSchema",
        "personalize:describeSolution",
        "personalize:describeSolutionVersion",
        "personalize:getPersonalizedRanking",
        "personalize:getRecommendations",
        "personalize:getSolutionMetrics",
        "personalize:listBatchInferenceJobs",
        "personalize:listBatchSegmentJobs",
        "personalize:listCampaigns",
        "personalize:listDataInsightsJobs",
        "personalize:listDatasetExportJobs",
        "personalize:listDatasetGroups",
        "personalize:listDatasetImportJobs",
        "personalize:listDatasets",
        "personalize:listEventTrackers",
        "personalize:listMetricAttributions",
        "personalize:listRecipes",
        "personalize:listRecommenders",
        "personalize:listSchemas",
        "personalize:listSolutions",
        "personalize:listSolutionVersions",
        "pipes:describePipe",
        "pipes:listPipes",
        "pipes:listTagsForResource",
        "polly:describeVoices",
```

```
        "polly:getLexicon",
        "polly:listLexicons",
        "pricing:describeServices",
        "pricing:getAttributeValues",
        "pricing:getProducts",
        "private-networks:getDeviceIdentifier",
        "private-networks:getNetwork",
        "private-networks:getNetworkResource",
        "private-networks:listDeviceIdentifiers",
        "private-networks:listNetworkResources",
        "private-networks:listNetworks",
        "qbusiness:getApplication",
        "qbusiness:getDataSource",
        "qbusiness:getIndex",
        "qbusiness:getRetriever",
        "qbusiness:getWebExperience",
        "qbusiness:listApplications",
        "qbusiness:listDataSources",
        "qbusiness:listDataSourceSyncJobs",
        "qbusiness:listIndices",
        "qbusiness:listRetrievers",
        "qbusiness:listWebExperiences",
        "quicksight:describeAccountCustomization",
        "quicksight:describeAccountCustomPermission",
        "quicksight:describeAccountSettings",
        "quicksight:describeAccountSubscription",
        "quicksight:describeAnalysis",
        "quicksight:describeAnalysisPermissions",
        "quicksight:describeCustomPermissions",
        "quicksight:describeDashboard",
        "quicksight:describeDashboardPermissions",
        "quicksight:describeDataSet",
        "quicksight:describeDataSetPermissions",
        "quicksight:describeDataSetRefreshProperties",
        "quicksight:describeDataSource",
        "quicksight:describeDataSourcePermissions",
        "quicksight:describeFolder",
        "quicksight:describeFolderPermissions",
        "quicksight:describeFolderResolvedPermissions",
        "quicksight:describeGroup",
        "quicksight:describeGroupMembership",
        "quicksight:describeIAMPolicyAssignment",
        "quicksight:describeIngestion",
        "quicksight:describeIpRestriction",
```

```
        "quicksight:describeNamespace",
        "quicksight:describeRefreshSchedule",
        "quicksight:describeRoleCustomPermission",
        "quicksight:describeTemplate",
        "quicksight:describeTemplateAlias",
        "quicksight:describeTemplatePermissions",
        "quicksight:describeTheme",
        "quicksight:describeThemeAlias",
        "quicksight:describeThemePermissions",
        "quicksight:describeTopic",
        "quicksight:describeTopicPermissions",
        "quicksight:describeTopicRefresh",
        "quicksight:describeTopicRefreshSchedule",
        "quicksight:describeUser",
        "quicksight:describeVPCConnection",
        "quicksight:listAnalyses",
        "quicksight:listCustomPermissions",
        "quicksight:listDashboards",
        "quicksight:listDashboardVersions",
        "quicksight:listDataSets",
        "quicksight:listDataSources",
        "quicksight:listFolderMembers",
        "quicksight:listFolders",
        "quicksight:listGroupMemberships",
        "quicksight:listGroups",
        "quicksight:listIAMPolicyAssignments",
        "quicksight:listIAMPolicyAssignmentsForUser",
        "quicksight:listIngestions",
        "quicksight:listNamespaces",
        "quicksight:listRefreshSchedules",
        "quicksight:listTemplateAliases",
        "quicksight:listTemplates",
        "quicksight:listTemplateVersions",
        "quicksight:listThemeAliases",
        "quicksight:listThemes",
        "quicksight:listThemeVersions",
        "quicksight:listTopicRefreshSchedules",
        "quicksight:listTopics",
        "quicksight:listUserGroups",
        "quicksight:listUsers",
        "quicksight:listVPCConnections",
        "quicksight:searchAnalyses",
        "quicksight:searchDashboards",
        "quicksight:searchDataSets",
```

```
        "quicksight:searchDataSources",
        "quicksight:searchFolders",
        "quicksight:searchGroups",
        "ram:getPermission",
        "ram:getResourceShareAssociations",
        "ram:getResourceShareInvitations",
        "ram:getResourceShares",
        "ram:listPendingInvitationResources",
        "ram:listPrincipals",
        "ram:listResources",
        "ram:listResourceSharePermissions",
        "rbin:getRule",
        "rbin:listRules",
        "rds:describeAccountAttributes",
        "rds:describeBlueGreenDeployments",
        "rds:describeCertificates",
        "rds:describeDBClusterAutomatedBackups",
        "rds:describeDBClusterBacktracks",
        "rds:describeDBClusterEndpoints",
        "rds:describeDBClusterParameterGroups",
        "rds:describeDBClusterParameters",
        "rds:describeDBClusters",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBClusterSnapshotAttributes",
        "rds:describeDBEngineVersions",
        "rds:describeDBInstanceAutomatedBackups",
        "rds:describeDBInstances",
        "rds:describeDBLogFiles",
        "rds:describeDBMajorEngineVersions",
        "rds:describeDBParameterGroups",
        "rds:describeDBParameters",
        "rds:describeDBProxies",
        "rds:describeDBProxyEndpoints",
        "rds:describeDBProxyTargetGroups",
        "rds:describeDBProxyTargets",
        "rds:describeDBRecommendations",
        "rds:describeDBSecurityGroups",
        "rds:describeDBShardGroups",
        "rds:describeDBSnapshotAttributes",
        "rds:describeDBSnapshots",
        "rds:describeDBSnapshotTenantDatabases",
        "rds:describeDBSubnetGroups",
        "rds:describeEngineDefaultClusterParameters",
        "rds:describeEngineDefaultParameters",
```

```
        "rds:describeEventCategories",
        "rds:describeEvents",
        "rds:describeEventSubscriptions",
        "rds:describeExportTasks",
        "rds:describeGlobalClusters",
        "rds:describeIntegrations",
        "rds:describeOptionGroupOptions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describePendingMaintenanceActions",
        "rds:describeReservedDBInstances",
        "rds:describeReservedDBInstancesOfferings",
        "rds:describeSourceRegions",
        "rds:describeTenantDatabases",
        "rds:describeValidDBInstanceModifications",
        "rds:listTagsForResource",
        "redshift-data:describeStatement",
        "redshift-data:listStatements",
        "redshift-serverless:getCustomDomainAssociation",
        "redshift-serverless:getEndpointAccess",
        "redshift-serverless:getNamespace",
        "redshift-serverless:getRecoveryPoint",
        "redshift-serverless:getReservation",
        "redshift-serverless:getReservationOffering",
        "redshift-serverless:getResourcePolicy",
        "redshift-serverless:getScheduledAction",
        "redshift-serverless:getSnapshot",
        "redshift-serverless:getTableRestoreStatus",
        "redshift-serverless:getTrack",
        "redshift-serverless:getUsageLimit",
        "redshift-serverless:getWorkgroup",
        "redshift-serverless:listCustomDomainAssociations",
        "redshift-serverless:listEndpointAccess",
        "redshift-serverless:listManagedWorkgroups",
        "redshift-serverless:listNamespaces",
        "redshift-serverless:listRecoveryPoints",
        "redshift-serverless:listReservationOfferings",
        "redshift-serverless:listReservations",
        "redshift-serverless:listScheduledActions",
        "redshift-serverless:listSnapshotCopyConfigurations",
        "redshift-serverless:listSnapshots",
        "redshift-serverless:listTableRestoreStatus",
        "redshift-serverless:listUsageLimits",
        "redshift-serverless:listWorkgroups",
```

```
        "redshift:describeClusterDbRevisions",
        "redshift:describeClusterParameterGroups",
        "redshift:describeClusterParameters",
        "redshift:describeClusters",
        "redshift:describeClusterSecurityGroups",
        "redshift:describeClusterSnapshots",
        "redshift:describeClusterSubnetGroups",
        "redshift:describeClusterTracks",
        "redshift:describeClusterVersions",
        "redshift:describeCustomDomainAssociations",
        "redshift:describeDataShares",
        "redshift:describeDataSharesForConsumer",
        "redshift:describeDataSharesForProducer",
        "redshift:describeDefaultClusterParameters",
        "redshift:describeEndpointAccess",
        "redshift:describeEndpointAuthorization",
        "redshift:describeEventCategories",
        "redshift:describeEvents",
        "redshift:describeEventSubscriptions",
        "redshift:describeHsmClientCertificates",
        "redshift:describeHsmConfigurations",
        "redshift:describeInboundIntegrations",
        "redshift:describeLoggingStatus",
        "redshift:describeNodeConfigurationOptions",
        "redshift:describeOrderableClusterOptions",
        "redshift:describeRedshiftIdcApplications",
        "redshift:describeReservedNodeOfferings",
        "redshift:describeReservedNodes",
        "redshift:describeResize",
        "redshift:describeSnapshotCopyGrants",
        "redshift:describeSnapshotSchedules",
        "redshift:describeStorage",
        "redshift:describeTableRestoreStatus",
        "redshift:describeTags",
        "redshift:describeUsageLimits",
        "rekognition:listCollections",
        "rekognition:listFaces",
        "resiliencehub:describeApp",
        "resiliencehub:describeAppAssessment",
        "resiliencehub:describeAppVersion",
        "resiliencehub:describeAppVersionAppComponent",
        "resiliencehub:describeAppVersionResource",
        "resiliencehub:describeAppVersionResourcesResolutionStatus",
        "resiliencehub:describeAppVersionTemplate",
```

```
        "resiliencehub:describeDraftAppVersionResourcesImportStatus",
        "resiliencehub:describeResiliencyPolicy",
        "resiliencehub:describeResourceGroupingRecommendationTask",
        "resiliencehub:listAlarmRecommendations",
        "resiliencehub:listAppAssessmentComplianceDrifts",
        "resiliencehub:listAppAssessmentResourceDrifts",
        "resiliencehub:listAppAssessments",
        "resiliencehub:listAppComponentCompliances",
        "resiliencehub:listAppComponentRecommendations",
        "resiliencehub:listAppInputSources",
        "resiliencehub:listApps",
        "resiliencehub:listAppVersionAppComponents",
        "resiliencehub:listAppVersionResourceMappings",
        "resiliencehub:listAppVersionResources",
        "resiliencehub:listAppVersions",
        "resiliencehub:listRecommendationTemplates",
        "resiliencehub:listResiliencyPolicies",
        "resiliencehub:listResourceGroupingRecommendations",
        "resiliencehub:listSopRecommendations",
        "resiliencehub:listSuggestedResiliencyPolicies",
        "resiliencehub:listTestRecommendations",
        "resiliencehub:listUnsupportedAppVersionResources",
        "resource-explorer-2:getAccountLevelServiceConfiguration",
        "resource-explorer-2:getIndex",
        "resource-explorer-2:getView",
        "resource-explorer-2:listIndexes",
        "resource-explorer-2:listViews",
        "resource-explorer-2:search",
        "resource-groups:getGroup",
        "resource-groups:getGroupQuery",
        "resource-groups:getTags",
        "resource-groups:listGroupResources",
        "resource-groups:listGroups",
        "resource-groups:searchResources",
        "robomaker:batchDescribeSimulationJob",
        "robomaker:describeDeploymentJob",
        "robomaker:describeFleet",
        "robomaker:describeRobot",
        "robomaker:describeRobotApplication",
        "robomaker:describeSimulationApplication",
        "robomaker:describeSimulationJob",
        "robomaker:listDeploymentJobs",
        "robomaker:listFleets",
        "robomaker:listRobotApplications",
```

```
        "robomaker:listRobots",
        "robomaker:listSimulationApplications",
        "robomaker:listSimulationJobs",
        "rolesanywhere:getProfile",
        "rolesanywhere:getTrustAnchor",
        "rolesanywhere:listProfiles",
        "rolesanywhere:listTrustAnchors",
        "route53-recovery-cluster:getRoutingControlState",
        "route53-recovery-cluster:listRoutingControls",
        "route53-recovery-control-config:describeCluster",
        "route53-recovery-control-config:describeControlPanel",
        "route53-recovery-control-config:describeRoutingControl",
        "route53-recovery-control-config:describeSafetyRule",
        "route53-recovery-control-config:getResourcePolicy",
        "route53-recovery-control-config:listAssociatedRoute53HealthChecks",
        "route53-recovery-control-config:listClusters",
        "route53-recovery-control-config:listControlPanels",
        "route53-recovery-control-config:listRoutingControls",
        "route53-recovery-control-config:listSafetyRules",
        "route53-recovery-readiness:getArchitectureRecommendations",
        "route53-recovery-readiness:getCell",
        "route53-recovery-readiness:getCellReadinessSummary",
        "route53-recovery-readiness:getReadinessCheck",
        "route53-recovery-readiness:getReadinessCheckResourceStatus",
        "route53-recovery-readiness:getReadinessCheckStatus",
        "route53-recovery-readiness:getRecoveryGroup",
        "route53-recovery-readiness:getRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:listCells",
        "route53-recovery-readiness:listReadinessChecks",
        "route53-recovery-readiness:listCrossAccountAuthorizations",
        "route53-recovery-readiness:listRecoveryGroups",
        "route53-recovery-readiness:listResourceSets",
        "route53-recovery-readiness:listRules",
        "route53:getAccountLimit",
        "route53:getChange",
        "route53:getCheckerIpRanges",
        "route53:getDNSSEC",
        "route53:getGeoLocation",
        "route53:getHealthCheck",
        "route53:getHealthCheckCount",
        "route53:getHealthCheckLastFailureReason",
        "route53:getHealthCheckStatus",
        "route53:getHostedZone",
        "route53:getHostedZoneCount",
```

```
        "route53:getHostedZoneLimit",
        "route53:getQueryLoggingConfig",
        "route53:getReusableDelegationSet",
        "route53:getTrafficPolicy",
        "route53:getTrafficPolicyInstance",
        "route53:getTrafficPolicyInstanceCount",
        "route53:listCidrBlocks",
        "route53:listCidrCollections",
        "route53:listCidrLocations",
        "route53:listGeoLocations",
        "route53:listHealthChecks",
        "route53:listHostedZones",
        "route53:listHostedZonesByName",
        "route53:listHostedZonesByVpc",
        "route53:listQueryLoggingConfigs",
        "route53:listResourceRecordSets",
        "route53:listReusableDelegationSets",
        "route53:listTrafficPolicies",
        "route53:listTrafficPolicyInstances",
        "route53:listTrafficPolicyInstancesByHostedZone",
        "route53:listTrafficPolicyInstancesByPolicy",
        "route53:listTrafficPolicyVersions",
        "route53:listVPCAssociationAuthorizations",
        "route53domains:checkDomainAvailability",
        "route53domains:getContactReachabilityStatus",
        "route53domains:getDomainDetail",
        "route53domains:getOperationDetail",
        "route53domains:listDomains",
        "route53domains:listOperations",
        "route53domains:listPrices",
        "route53domains:listTagsForDomain",
        "route53domains:viewBilling",
        "route53profiles:getProfile",
        "route53profiles:getProfileAssociation",
        "route53profiles:getProfileResourceAssociation",
        "route53profiles:listProfileAssociations",
        "route53profiles:listProfileResourceAssociations",
        "route53profiles:listProfiles",
        "route53profiles:listTagsForResource",
        "route53resolver:getFirewallConfig",
        "route53resolver:getFirewallDomainList",
        "route53resolver:getFirewallRuleGroup",
        "route53resolver:getFirewallRuleGroupAssociation",
        "route53resolver:getFirewallRuleGroupPolicy",
```

```
        "route53resolver:getOutpostResolver",
        "route53resolver:getResolverConfig",
        "route53resolver:getResolverDnssecConfig",
        "route53resolver:getResolverEndpoint",
        "route53resolver:getResolverQueryLogConfig",
        "route53resolver:getResolverQueryLogConfigAssociation",
        "route53resolver:getResolverQueryLogConfigPolicy",
        "route53resolver:getResolverRule",
        "route53resolver:getResolverRuleAssociation",
        "route53resolver:getResolverRulePolicy",
        "route53resolver:listFirewallConfigs",
        "route53resolver:listFirewallDomainLists",
        "route53resolver:listFirewallDomains",
        "route53resolver:listFirewallRuleGroupAssociations",
        "route53resolver:listFirewallRuleGroups",
        "route53resolver:listFirewallRules",
        "route53resolver:listOutpostResolvers",
        "route53resolver:listResolverConfigs",
        "route53resolver:listResolverDnssecConfigs",
        "route53resolver:listResolverEndpointIpAddresses",
        "route53resolver:listResolverEndpoints",
        "route53resolver:listResolverQueryLogConfigAssociations",
        "route53resolver:listResolverQueryLogConfigs",
        "route53resolver:listResolverRuleAssociations",
        "route53resolver:listResolverRules",
        "route53resolver:listTagsForResource",
        "route53globalresolver:getAccessSource",
        "route53globalresolver:getAccessToken",
        "route53globalresolver:getDNSView",
        "route53globalresolver:getFirewallDomainList",
        "route53globalresolver:getFirewallRule",
        "route53globalresolver:getGlobalResolver",
        "route53globalresolver:getHostedZoneAssociation",
        "route53globalresolver:getManagedFirewallDomainList",
        "route53globalresolver:listAccessSources",
        "route53globalresolver:listAccessTokens",
        "route53globalresolver:listDNSViews",
        "route53globalresolver:listFirewallDomainLists",
        "route53globalresolver:listFirewallDomains",
        "route53globalresolver:listFirewallRules",
        "route53globalresolver:listGlobalResolvers",
        "route53globalresolver:listHostedZoneAssociations",
        "route53globalresolver:listManagedFirewallDomainLists",
        "rum:batchGetRumMetricDefinitions",
```

```
        "rum:getAppMonitor",
        "rum:listAppMonitors",
        "rum:listRumMetricsDestinations",
        "s3-outposts:getLifecycleConfiguration",
        "s3-outposts:getAccessPoint",
        "s3-outposts:getAccessPointPolicy",
        "s3-outposts:getBucketPolicy",
        "s3-outposts:getBucketVersioning",
        "s3-outposts:getReplicationConfiguration",
        "s3-outposts:listAccessPoints",
        "s3-outposts:listEndpoints",
        "s3-outposts:listOutpostsWithS3",
        "s3-outposts:listRegionalBuckets",
        "s3-outposts:listSharedEndpoints",
        "s3:describeJob",
        "s3:describeMultiRegionAccessPointOperation",
        "s3:getAccelerateConfiguration",
        "s3:getAccessGrant",
        "s3:getAccessGrantsInstance",
        "s3:getAccessGrantsInstanceResourcePolicy",
        "s3:getAccessGrantsLocation",
        "s3:getAccessPoint",
        "s3:getAccessPointConfigurationForObjectLambda",
        "s3:getAccessPointForObjectLambda",
        "s3:getAccessPointPolicy",
        "s3:getAccessPointPolicyForObjectLambda",
        "s3:getAccessPointPolicyStatus",
        "s3:getAccessPointPolicyStatusForObjectLambda",
        "s3:getAccountPublicAccessBlock",
        "s3:getAnalyticsConfiguration",
        "s3:getBucketAcl",
        "s3:getBucketCORS",
        "s3:getBucketLocation",
        "s3:getBucketLogging",
        "s3:getBucketNotification",
        "s3:getBucketObjectLockConfiguration",
        "s3:getBucketOwnershipControls",
        "s3:getBucketPolicy",
        "s3:getBucketPolicyStatus",
        "s3:getBucketPublicAccessBlock",
        "s3:getBucketRequestPayment",
        "s3:getBucketVersioning",
        "s3:getBucketWebsite",
        "s3:getEncryptionConfiguration",
```

```
        "s3:getIntelligentTieringConfiguration",
        "s3:getInventoryConfiguration",
        "s3:getLifecycleConfiguration",
        "s3:getMetricsConfiguration",
        "s3:getMultiRegionAccessPoint",
        "s3:getMultiRegionAccessPointPolicy",
        "s3:getMultiRegionAccessPointPolicyStatus",
        "s3:getMultiRegionAccessPointRoutes",
        "s3:getObjectAcl",
        "s3:getObjectLegalHold",
        "s3:getObjectRetention",
        "s3:getReplicationConfiguration",
        "s3:getStorageLensConfiguration",
        "s3:listAccessGrants",
        "s3:listAccessGrantsInstances",
        "s3:listAccessGrantsLocations",
        "s3:listAccessPoints",
        "s3:listAccessPointsForObjectLambda",
        "s3:listAllMyBuckets",
        "s3:listBucket",
        "s3:listBucketMultipartUploads",
        "s3:listBucketVersions",
        "s3:listJobs",
        "s3:listMultipartUploadParts",
        "s3:listMultiRegionAccessPoints",
        "s3:listStorageLensConfigurations",
        "s3express:getBucketPolicy",
        "s3express:listAllMyDirectoryBuckets",
        "s3files:getAccessPoint",
        "s3files:getFileSystem",
        "s3files:getFileSystemPolicy",
        "s3files:getMountTarget",
        "s3files:getSynchronizationConfiguration",
        "s3files:listAccessPoints",
        "s3files:listFileSystems",
        "s3files:listMountTargets",
        "s3files:listTagsForResource",
        "s3tables:getNamespace",
        "s3tables:getTable",
        "s3tables:getTableBucket",
        "s3tables:getTableBucketEncryption",
        "s3tables:getTableBucketMaintenanceConfiguration",
        "s3tables:getTableBucketMetricsConfiguration",
        "s3tables:getTableBucketPolicy",
```

```
        "s3tables:getTableBucketReplication",
        "s3tables:getTableBucketStorageClass",
        "s3tables:getTableEncryption",
        "s3tables:getTableMaintenanceConfiguration",
        "s3tables:getTableMaintenanceJobStatus",
        "s3tables:getTableMetadataLocation",
        "s3tables:getTablePolicy",
        "s3tables:getTableRecordExpirationConfiguration",
        "s3tables:getTableRecordExpirationJobStatus",
        "s3tables:getTableReplication",
        "s3tables:getTableReplicationStatus",
        "s3tables:getTableStorageClass",
        "s3tables:listNamespaces",
        "s3tables:listTableBuckets",
        "s3tables:listTables",
        "s3vectors:getIndex",
        "s3vectors:getVectorBucket",
        "s3vectors:getVectorBucketPolicy",
        "s3vectors:listIndexes",
        "s3vectors:listVectorBuckets",
        "sagemaker:describeAction",
        "sagemaker:describeAlgorithm",
        "sagemaker:describeApp",
        "sagemaker:describeAppImageConfig",
        "sagemaker:describeArtifact",
        "sagemaker:describeAutoMLJob",
        "sagemaker:describeAutoMLJobV2",
        "sagemaker:describeCluster",
        "sagemaker:describeClusterNode",
        "sagemaker:describeClusterEvent",
        "sagemaker:describeClusterSchedulerConfig",
        "sagemaker:describeCodeRepository",
        "sagemaker:describeCompilationJob",
        "sagemaker:describeComputeQuota",
        "sagemaker:describeContext",
        "sagemaker:describeDataQualityJobDefinition",
        "sagemaker:describeDevice",
        "sagemaker:describeDeviceFleet",
        "sagemaker:describeDomain",
        "sagemaker:describeEdgeDeploymentPlan",
        "sagemaker:describeEdgePackagingJob",
        "sagemaker:describeEndpoint",
        "sagemaker:describeEndpointConfig",
        "sagemaker:describeExperiment",
```

```
        "sagemaker:describeFeatureGroup",
        "sagemaker:describeFeatureMetadata",
        "sagemaker:describeFlowDefinition",
        "sagemaker:describeHub",
        "sagemaker:describeHubContent",
        "sagemaker:describeHumanTaskUi",
        "sagemaker:describeHyperParameterTuningJob",
        "sagemaker:describeImage",
        "sagemaker:describeImageVersion",
        "sagemaker:describeInferenceComponent",
        "sagemaker:describeInferenceExperiment",
        "sagemaker:describeInferenceRecommendationsJob",
        "sagemaker:describeLabelingJob",
        "sagemaker:describeLineageGroup",
        "sagemaker:describeMlflowApp",
        "sagemaker:describeMlflowTrackingServer",
        "sagemaker:describeModel",
        "sagemaker:describeModelBiasJobDefinition",
        "sagemaker:describeModelCard",
        "sagemaker:describeModelCardExportJob",
        "sagemaker:describeModelExplainabilityJobDefinition",
        "sagemaker:describeModelPackage",
        "sagemaker:describeModelPackageGroup",
        "sagemaker:describeModelQualityJobDefinition",
        "sagemaker:describeMonitoringSchedule",
        "sagemaker:describeNotebookInstance",
        "sagemaker:describeNotebookInstanceLifecycleConfig",
        "sagemaker:describeOptimizationJob",
        "sagemaker:describePipeline",
        "sagemaker:describePipelineDefinitionForExecution",
        "sagemaker:describePipelineExecution",
        "sagemaker:describePartnerApp",
        "sagemaker:describeProcessingJob",
        "sagemaker:describeProject",
        "sagemaker:describeReservedCapacity",
        "sagemaker:describeSpace",
        "sagemaker:describeStudioLifecycleConfig",
        "sagemaker:describeSubscribedWorkteam",
        "sagemaker:describeTrainingJob",
        "sagemaker:describeTrainingPlan",
        "sagemaker:describeTransformJob",
        "sagemaker:describeTrial",
        "sagemaker:describeTrialComponent",
        "sagemaker:describeUserProfile",
```

```
        "sagemaker:describeWorkforce",
        "sagemaker:describeWorkteam",
        "sagemaker:getDeviceFleetReport",
        "sagemaker:getModelPackageGroupPolicy",
        "sagemaker:getLineageGroupPolicy",
        "sagemaker:getSagemakerServicecatalogPortfolioStatus",
        "sagemaker:listActions",
        "sagemaker:listAlgorithms",
        "sagemaker:listAliases",
        "sagemaker:listAppImageConfigs",
        "sagemaker:listApps",
        "sagemaker:listArtifacts",
        "sagemaker:listAssociations",
        "sagemaker:listAutoMLJobs",
        "sagemaker:listCandidatesForAutoMLJob",
        "sagemaker:listClusterNodes",
        "sagemaker:listClusters",
        "sagemaker:listClusterEvents",
        "sagemaker:listClusterSchedulerConfigs",
        "sagemaker:listCodeRepositories",
        "sagemaker:listCompilationJobs",
        "sagemaker:listComputeQuotas",
        "sagemaker:listContexts",
        "sagemaker:listDataQualityJobDefinitions",
        "sagemaker:listDeviceFleets",
        "sagemaker:listDevices",
        "sagemaker:listDomains",
        "sagemaker:listEdgeDeploymentPlans",
        "sagemaker:listEdgePackagingJobs",
        "sagemaker:listEndpointConfigs",
        "sagemaker:listEndpoints",
        "sagemaker:listExperiments",
        "sagemaker:listFeatureGroups",
        "sagemaker:listFlowDefinitions",
        "sagemaker:listHubContents",
        "sagemaker:listHubContentVersions",
        "sagemaker:listHubs",
        "sagemaker:listHumanTaskUis",
        "sagemaker:listHyperParameterTuningJobs",
        "sagemaker:listImages",
        "sagemaker:listImageVersions",
        "sagemaker:listInferenceComponents",
        "sagemaker:listInferenceExperiments",
        "sagemaker:listInferenceRecommendationsJobs",
```

```
        "sagemaker:listInferenceRecommendationsJobSteps",
        "sagemaker:listLabelingJobs",
        "sagemaker:listLabelingJobsForWorkteam",
        "sagemaker:listLineageGroups",
        "sagemaker:listMlflowApps",
        "sagemaker:listMlflowTrackingServers",
        "sagemaker:listModelBiasJobDefinitions",
        "sagemaker:listModelCardExportJobs",
        "sagemaker:listModelCards",
        "sagemaker:listModelCardVersions",
        "sagemaker:listModelExplainabilityJobDefinitions",
        "sagemaker:listModelMetadata",
        "sagemaker:listModelPackageGroups",
        "sagemaker:listModelPackages",
        "sagemaker:listModelQualityJobDefinitions",
        "sagemaker:listModels",
        "sagemaker:listMonitoringAlertHistory",
        "sagemaker:listMonitoringAlerts",
        "sagemaker:listMonitoringExecutions",
        "sagemaker:listMonitoringSchedules",
        "sagemaker:listNotebookInstanceLifecycleConfigs",
        "sagemaker:listNotebookInstances",
        "sagemaker:listOptimizationJobs",
        "sagemaker:listPartnerApps",
        "sagemaker:listPipelineExecutions",
        "sagemaker:listPipelineExecutionSteps",
        "sagemaker:listPipelineParametersForExecution",
        "sagemaker:listPipelines",
        "sagemaker:listPipelineVersions",
        "sagemaker:listProcessingJobs",
        "sagemaker:listProjects",
        "sagemaker:listResourceCatalogs",
        "sagemaker:listSpaces",
        "sagemaker:listStageDevices",
        "sagemaker:listStudioLifecycleConfigs",
        "sagemaker:listSubscribedWorkteams",
        "sagemaker:listTags",
        "sagemaker:listTrainingJobs",
        "sagemaker:listTrainingJobsForHyperParameterTuningJob",
        "sagemaker:listTrainingPlans",
        "sagemaker:listTransformJobs",
        "sagemaker:listTrialComponents",
        "sagemaker:listTrials",
        "sagemaker:listUserProfiles",
```

```
        "sagemaker:listUltraServersByReservedCapacity",
        "sagemaker:listWorkforces",
        "sagemaker:listWorkteams",
        "sagemaker:search",
        "savingsplans:describeSavingsPlanRates",
        "savingsplans:describeSavingsPlans",
        "savingsplans:describeSavingsPlansOfferingRates",
        "savingsplans:describeSavingsPlansOfferings",
        "scheduler:getSchedule",
        "scheduler:getScheduleGroup",
        "scheduler:listScheduleGroups",
        "scheduler:listSchedules",
        "schemas:describeCodeBinding",
        "schemas:describeDiscoverer",
        "schemas:describeRegistry",
        "schemas:describeSchema",
        "schemas:getCodeBindingSource",
        "schemas:getDiscoveredSchema",
        "schemas:getResourcePolicy",
        "schemas:listDiscoverers",
        "schemas:listRegistries",
        "schemas:listSchemas",
        "schemas:listSchemaVersions",
        "sdb:domainMetadata",
        "sdb:listDomains",
        "secretsmanager:describeSecret",
        "secretsmanager:getResourcePolicy",
        "secretsmanager:listSecrets",
        "secretsmanager:listSecretVersionIds",
        "security-ir:batchGetMemberAccountDetails",
        "security-ir:getMembership",
        "security-ir:listCases",
        "security-ir:listMemberships",
        "securityhub:batchGetAutomationRules",
        "securityhub:batchGetConfigurationPolicyAssociations",
        "securityhub:describeHub",
        "securityhub:describeOrganizationConfiguration",
        "securityhub:describeProductsV2",
        "securityhub:describeSecurityHubV2",
        "securityhub:getConfigurationPolicy",
        "securityhub:getConfigurationPolicyAssociation",
        "securityhub:getEnabledStandards",
        "securityhub:getFindingAggregator",
        "securityhub:getFindingHistory",
```

```
        "securityhub:getFindings",
        "securityhub:getInsightResults",
        "securityhub:getInsights",
        "securityhub:getMasterAccount",
        "securityhub:getMembers",
        "securityhub:getAggregatorV2",
        "securityhub:getAutomationRuleV2",
        "securityhub:getConnectorV2",
        "securityhub:getResourcesV2",
        "securityhub:listAutomationRules",
        "securityhub:listConfigurationPolicies",
        "securityhub:listConfigurationPolicyAssociations",
        "securityhub:listEnabledProductsForImport",
        "securityhub:listFindingAggregators",
        "securityhub:listInvitations",
        "securityhub:listMembers",
        "securityhub:listAggregatorsV2",
        "securityhub:listAutomationRulesV2",
        "securityhub:listConnectorsV2",
        "securitylake:getDataLakeExceptionSubscription",
        "securitylake:getDataLakeOrganizationConfiguration",
        "securitylake:getDataLakeSources",
        "securitylake:getSubscriber",
        "securitylake:listDataLakeExceptions",
        "securitylake:listDataLakes",
        "securitylake:listLogSources",
        "securitylake:listSubscribers",
        "serverlessrepo:getApplication",
        "serverlessrepo:getApplicationPolicy",
        "serverlessrepo:getCloudFormationTemplate",
        "serverlessrepo:listApplicationDependencies",
        "serverlessrepo:listApplications",
        "serverlessrepo:listApplicationVersions",
        "servicecatalog:describeConstraint",
        "servicecatalog:describePortfolio",
        "servicecatalog:describeProduct",
        "servicecatalog:describeProductAsAdmin",
        "servicecatalog:describeProductView",
        "servicecatalog:describeProvisioningArtifact",
        "servicecatalog:describeProvisioningParameters",
        "servicecatalog:describeRecord",
        "servicecatalog:listAcceptedPortfolioShares",
        "servicecatalog:listConstraintsForPortfolio",
        "servicecatalog:listLaunchPaths",
```

```
        "servicecatalog:listPortfolioAccess",
        "servicecatalog:listPortfolios",
        "servicecatalog:listPortfoliosForProduct",
        "servicecatalog:listPrincipalsForPortfolio",
        "servicecatalog:listProvisioningArtifacts",
        "servicecatalog:listRecordHistory",
        "servicecatalog:scanProvisionedProducts",
        "servicecatalog:searchProducts",
        "servicequotas:getAssociationForServiceQuotaTemplate",
        "servicequotas:getAWSDefaultServiceQuota",
        "servicequotas:getRequestedServiceQuotaChange",
        "servicequotas:getServiceQuota",
        "servicequotas:getServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:listAWSDefaultServiceQuotas",
        "servicequotas:listRequestedServiceQuotaChangeHistory",
        "servicequotas:listRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:listServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:listServiceQuotas",
        "servicequotas:listServices",
        "ses:batchGetMetricData",
        "ses:describeActiveReceiptRuleSet",
        "ses:describeConfigurationSet",
        "ses:describeReceiptRule",
        "ses:describeReceiptRuleSet",
        "ses:getAccount",
        "ses:getAccountSendingEnabled",
        "ses:getAddonInstance",
        "ses:getAddonSubscription",
        "ses:getArchive",
        "ses:getArchiveExport",
        "ses:getArchiveSearch",
        "ses:getArchiveSearchResults",
        "ses:getBlacklistReports",
        "ses:getConfigurationSet",
        "ses:getConfigurationSetEventDestinations",
        "ses:getContactList",
        "ses:getDedicatedIp",
        "ses:getDedicatedIpPool",
        "ses:getDedicatedIps",
        "ses:getDeliverabilityDashboardOptions",
        "ses:getDeliverabilityTestReport",
        "ses:getDomainDeliverabilityCampaign",
        "ses:getDomainStatisticsReport",
        "ses:getEmailIdentity",
```

```
        "ses:getIdentityDkimAttributes",
        "ses:getIdentityMailFromDomainAttributes",
        "ses:getIdentityNotificationAttributes",
        "ses:getIdentityPolicies",
        "ses:getIdentityVerificationAttributes",
        "ses:getImportJob",
        "ses:getIngressPoint",
        "ses:getMessageInsights",
        "ses:getRelay",
        "ses:getRuleSet",
        "ses:getTrafficPolicy",
        "ses:getSendQuota",
        "ses:getSendStatistics",
        "ses:listConfigurationSets",
        "ses:listAddonInstances",
        "ses:listAddonSubscriptions",
        "ses:listArchiveExports",
        "ses:listArchives",
        "ses:listArchiveSearches",
        "ses:listContactLists",
        "ses:listContacts",
        "ses:listCustomVerificationEmailTemplates",
        "ses:listDedicatedIpPools",
        "ses:listDeliverabilityTestReports",
        "ses:listDomainDeliverabilityCampaigns",
        "ses:listEmailIdentities",
        "ses:listEmailTemplates",
        "ses:listIdentities",
        "ses:listIdentityPolicies",
        "ses:listImportJobs",
        "ses:listIngressPoints",
        "ses:listReceiptFilters",
        "ses:listReceiptRuleSets",
        "ses:listRelays",
        "ses:listRuleSets",
        "ses:listRecommendations",
        "ses:listTagsForResource",
        "ses:listTemplates",
        "ses:listTrafficPolicies",
        "ses:listVerifiedEmailAddresses",
        "shield:describeAttack",
        "shield:describeAttackStatistics",
        "shield:describeDRTAccess",
        "shield:describeProtection",
```

```
        "shield:describeProtectionGroup",
        "shield:describeSubscription",
        "shield:getSubscriptionState",
        "shield:listAttacks",
        "shield:listProtectionGroups",
        "shield:listProtections",
        "signer:describeSigningJob",
        "signer:getRevocationStatus",
        "signer:getSigningPlatform",
        "signer:getSigningProfile",
        "signer:listProfilePermissions",
        "signer:listSigningJobs",
        "signer:listSigningPlatforms",
        "signer:listSigningProfiles",
        "sms-voice:describeAccountAttributes",
        "sms-voice:describeSpendLimits",
        "sms-voice:describeVerifiedDestinationNumbers",
        "sms-voice:getConfigurationSetEventDestinations",
        "sms:getConnectors",
        "sms:getReplicationJobs",
        "sms:getReplicationRuns",
        "sms:getServers",
        "snowball:describeAddress",
        "snowball:describeAddresses",
        "snowball:describeJob",
        "snowball:getSnowballUsage",
        "snowball:listJobs",
        "snowball:listServiceVersions",
        "sns:checkIfPhoneNumberIsOptedOut",
        "sns:getDataProtectionPolicy",
        "sns:getEndpointAttributes",
        "sns:getPlatformApplicationAttributes",
        "sns:getSMSAttributes",
        "sns:getSMSSandboxAccountStatus",
        "sns:getSubscriptionAttributes",
        "sns:getTopicAttributes",
        "sns:listEndpointsByPlatformApplication",
        "sns:listOriginationNumbers",
        "sns:listPhoneNumbersOptedOut",
        "sns:listPlatformApplications",
        "sns:listSMSSandboxPhoneNumbers",
        "sns:listSubscriptions",
        "sns:listSubscriptionsByTopic",
        "sns:listTopics",
```

```
        "sqs:getQueueAttributes",
        "sqs:getQueueUrl",
        "sqs:listDeadLetterSourceQueues",
        "sqs:listMessageMoveTasks",
        "sqs:listQueues",
        "ssm-contacts:describeEngagement",
        "ssm-contacts:describePage",
        "ssm-contacts:getContact",
        "ssm-contacts:getContactChannel",
        "ssm-contacts:getContactPolicy",
        "ssm-contacts:getRotation",
        "ssm-contacts:getRotationOverride",
        "ssm-contacts:listContactChannels",
        "ssm-contacts:listContacts",
        "ssm-contacts:listEngagements",
        "ssm-contacts:listPageReceipts",
        "ssm-contacts:listPageResolutions",
        "ssm-contacts:listPagesByContact",
        "ssm-contacts:listPagesByEngagement",
        "ssm-contacts:listPreviewRotationShifts",
        "ssm-contacts:listRotationOverrides",
        "ssm-contacts:listRotations",
        "ssm-contacts:listRotationShifts",
        "ssm-incidents:batchGetIncidentFindings",
        "ssm-incidents:getIncidentRecord",
        "ssm-incidents:getReplicationSet",
        "ssm-incidents:getResourcePolicies",
        "ssm-incidents:getResponsePlan",
        "ssm-incidents:getTimelineEvent",
        "ssm-incidents:listIncidentFindings",
        "ssm-incidents:listIncidentRecords",
        "ssm-incidents:listRelatedItems",
        "ssm-incidents:listReplicationSets",
        "ssm-incidents:listResponsePlans",
        "ssm-incidents:listTimelineEvents",
        "ssm-quicksetup:getConfiguration",
        "ssm-quicksetup:getConfigurationManager",
        "ssm-quicksetup:getServiceSettings",
        "ssm-quicksetup:listConfigurationManagers",
        "ssm-quicksetup:listConfigurations",
        "ssm-quicksetup:listQuickSetupTypes",
        "ssm-sap:getApplication",
        "ssm-sap:getComponent",
        "ssm-sap:getConfigurationCheckOperation",
```

```
        "ssm-sap:getDatabase",
        "ssm-sap:getOperation",
        "ssm-sap:getResourcePermission",
        "ssm-sap:listApplications",
        "ssm-sap:listComponents",
        "ssm-sap:listConfigurationCheckDefinitions",
        "ssm-sap:listConfigurationCheckOperations",
        "ssm-sap:listDatabases",
        "ssm-sap:listOperations",
        "ssm-sap:listSubCheckResults",
        "ssm-sap:listSubCheckRuleResults",
        "ssm:describeActivations",
        "ssm:describeAssociation",
        "ssm:describeAssociationExecutions",
        "ssm:describeAssociationExecutionTargets",
        "ssm:describeAutomationExecutions",
        "ssm:describeAutomationStepExecutions",
        "ssm:describeAvailablePatches",
        "ssm:describeDocument",
        "ssm:describeDocumentPermission",
        "ssm:describeEffectiveInstanceAssociations",
        "ssm:describeEffectivePatchesForPatchBaseline",
        "ssm:describeInstanceAssociationsStatus",
        "ssm:describeInstanceInformation",
        "ssm:describeInstancePatches",
        "ssm:describeInstancePatchStates",
        "ssm:describeInstancePatchStatesForPatchGroup",
        "ssm:describeInstanceProperties",
        "ssm:describeInventoryDeletions",
        "ssm:describeMaintenanceWindowExecutions",
        "ssm:describeMaintenanceWindowExecutionTaskInvocations",
        "ssm:describeMaintenanceWindowExecutionTasks",
        "ssm:describeMaintenanceWindows",
        "ssm:describeMaintenanceWindowSchedule",
        "ssm:describeMaintenanceWindowsForTarget",
        "ssm:describeMaintenanceWindowTargets",
        "ssm:describeMaintenanceWindowTasks",
        "ssm:describeOpsItems",
        "ssm:describeParameters",
        "ssm:describePatchBaselines",
        "ssm:describePatchGroups",
        "ssm:describePatchGroupState",
        "ssm:describePatchProperties",
        "ssm:describeSessions",
```

```
        "ssm:getAutomationExecution",
        "ssm:getCalendarState",
        "ssm:getCommandInvocation",
        "ssm:getConnectionStatus",
        "ssm:getDefaultPatchBaseline",
        "ssm:getDeployablePatchSnapshotForInstance",
        "ssm:getInventorySchema",
        "ssm:getMaintenanceWindow",
        "ssm:getMaintenanceWindowExecution",
        "ssm:getMaintenanceWindowExecutionTask",
        "ssm:getMaintenanceWindowExecutionTaskInvocation",
        "ssm:getMaintenanceWindowTask",
        "ssm:getOpsItem",
        "ssm:getOpsMetadata",
        "ssm:getOpsSummary",
        "ssm:getPatchBaseline",
        "ssm:getPatchBaselineForPatchGroup",
        "ssm:getResourcePolicies",
        "ssm:getServiceSetting",
        "ssm:listAssociations",
        "ssm:listAssociationVersions",
        "ssm:listCommandInvocations",
        "ssm:listCommands",
        "ssm:listComplianceItems",
        "ssm:listComplianceSummaries",
        "ssm:listDocumentMetadataHistory",
        "ssm:listDocuments",
        "ssm:listDocumentVersions",
        "ssm:listNodes",
        "ssm:listNodesSummary",
        "ssm:listOpsItemEvents",
        "ssm:listOpsItemRelatedItems",
        "ssm:listOpsMetadata",
        "ssm:listResourceComplianceSummaries",
        "ssm:listResourceDataSync",
        "ssm:listTagsForResource",
        "sso:describeApplication",
        "sso:describeApplicationAssignment",
        "sso:describeApplicationProvider",
        "sso:describeAccountAssignmentCreationStatus",
        "sso:describeAccountAssignmentDeletionStatus",
        "sso:describeInstance",
        "sso:describeInstanceAccessControlAttributeConfiguration",
        "sso:describePermissionSet",
```

```
        "sso:describePermissionSetProvisioningStatus",
        "sso:describeTrustedTokenIssuer",
        "sso:getApplicationAccessScope",
        "sso:getApplicationAssignmentConfiguration",
        "sso:getApplicationAuthenticationMethod",
        "sso:getApplicationGrant",
        "sso:getApplicationInstance",
        "sso:getApplicationTemplate",
        "sso:getInlinePolicyForPermissionSet",
        "sso:getManagedApplicationInstance",
        "sso:getPermissionsBoundaryForPermissionSet",
        "sso:getSharedSsoConfiguration",
        "sso:listApplicationAccessScopes",
        "sso:listApplicationAssignments",
        "sso:listApplicationAuthenticationMethods",
        "sso:listApplicationGrants",
        "sso:listApplicationInstances",
        "sso:listApplicationProviders",
        "sso:listApplications",
        "sso:listApplicationTemplates",
        "sso:listAccountAssignmentCreationStatus",
        "sso:listAccountAssignmentDeletionStatus",
        "sso:listAccountAssignments",
        "sso:listAccountAssignmentsForPrincipal",
        "sso:listAccountsForProvisionedPermissionSet",
        "sso:listApplicationAssignmentsForPrincipal",
        "sso:listCustomerManagedPolicyReferencesInPermissionSet",
        "sso:listDirectoryAssociations",
        "sso:listInstances",
        "sso:listManagedPoliciesInPermissionSet",
        "sso:listPermissionSetProvisioningStatus",
        "sso:listPermissionSets",
        "sso:listPermissionSetsProvisionedToAccount",
        "sso:listProfileAssociations",
        "sso:listTrustedTokenIssuers",
        "states:describeActivity",
        "states:describeExecution",
        "states:describeMapRun",
        "states:describeStateMachine",
        "states:describeStateMachineAlias",
        "states:describeStateMachineForExecution",
        "states:getExecutionHistory",
        "states:listActivities",
        "states:listExecutions",
```

```
        "states:listMapRuns",
        "states:listStateMachineAliases",
        "states:listStateMachines",
        "states:listStateMachineVersions",
        "storagegateway:describeBandwidthRateLimit",
        "storagegateway:describeCache",
        "storagegateway:describeCachediSCSIVolumes",
        "storagegateway:describeFileSystemAssociations",
        "storagegateway:describeGatewayInformation",
        "storagegateway:describeMaintenanceStartTime",
        "storagegateway:describeNFSFileShares",
        "storagegateway:describeSMBFileShares",
        "storagegateway:describeSMBSettings",
        "storagegateway:describeSnapshotSchedule",
        "storagegateway:describeStorediSCSIVolumes",
        "storagegateway:describeTapeArchives",
        "storagegateway:describeTapeRecoveryPoints",
        "storagegateway:describeTapes",
        "storagegateway:describeUploadBuffer",
        "storagegateway:describeVTLDevices",
        "storagegateway:describeWorkingStorage",
        "storagegateway:listAutomaticTapeCreationPolicies",
        "storagegateway:listFileShares",
        "storagegateway:listFileSystemAssociations",
        "storagegateway:listGateways",
        "storagegateway:listLocalDisks",
        "storagegateway:listTagsForResource",
        "storagegateway:listTapes",
        "storagegateway:listVolumeInitiators",
        "storagegateway:listVolumeRecoveryPoints",
        "storagegateway:listVolumes",
        "sts:getCallerIdentity",
        "swf:countClosedWorkflowExecutions",
        "swf:countOpenWorkflowExecutions",
        "swf:countPendingActivityTasks",
        "swf:countPendingDecisionTasks",
        "swf:describeActivityType",
        "swf:describeDomain",
        "swf:describeWorkflowExecution",
        "swf:describeWorkflowType",
        "swf:getWorkflowExecutionHistory",
        "swf:listActivityTypes",
        "swf:listClosedWorkflowExecutions",
        "swf:listDomains",
```

```
        "swf:listOpenWorkflowExecutions",
        "swf:listWorkflowTypes",
        "sustainability:getEstimatedCarbonEmissions",
        "sustainability:getEstimatedCarbonEmissionsDimensionValues",
        "sustainability:getEstimatedWaterAllocation",
        "sustainability:getEstimatedWaterAllocationDimensionValues",
        "synthetics:describeCanaries",
        "synthetics:describeCanariesLastRun",
        "synthetics:describeRuntimeVersions",
        "synthetics:getCanary",
        "synthetics:getCanaryRuns",
        "synthetics:getGroup",
        "synthetics:listAssociatedGroups",
        "synthetics:listGroupResources",
        "synthetics:listGroups",
        "tax:getTaxInheritance",
        "tax:getTaxRegistration",
        "thinclient:getDevice",
        "thinclient:getEnvironment",
        "thinclient:getSoftwareSet",
        "thinclient:listDevices",
        "thinclient:listEnvironments",
        "thinclient:listSoftwareSets",
        "timestream:describeAccountSettings",
        "timestream:describeBatchLoadTask",
        "timestream:describeDatabase",
        "timestream:describeEndpoints",
        "timestream:describeScheduledQuery",
        "timestream:describeTable",
        "timestream:listBatchLoadTasks",
        "timestream:listDatabases",
        "timestream:listScheduledQueries",
        "timestream:listTables",
        "tiros:createQuery",
        "tiros:getQueryAnswer",
        "tiros:getQueryExplanation",
        "tnb:getSolFunctionInstance",
        "tnb:getSolFunctionPackage",
        "tnb:getSolNetworkInstance",
        "tnb:getSolNetworkOperation",
        "tnb:getSolNetworkPackage",
        "tnb:listSolFunctionInstances",
        "tnb:listSolFunctionPackages",
        "tnb:listSolNetworkInstances",
```

```
        "tnb:listSolNetworkOperations",
        "tnb:listSolNetworkPackages",
        "transcribe:describeLanguageModel",
        "transcribe:getCallAnalyticsCategory",
        "transcribe:getCallAnalyticsJob",
        "transcribe:getMedicalTranscriptionJob",
        "transcribe:getMedicalVocabulary",
        "transcribe:getTranscriptionJob",
        "transcribe:getVocabulary",
        "transcribe:getVocabularyFilter",
        "transcribe:listCallAnalyticsCategories",
        "transcribe:listCallAnalyticsJobs",
        "transcribe:listLanguageModels",
        "transcribe:listMedicalTranscriptionJobs",
        "transcribe:listMedicalVocabularies",
        "transcribe:listTranscriptionJobs",
        "transcribe:listVocabularies",
        "transcribe:listVocabularyFilters",
        "transfer:describeAccess",
        "transfer:describeAgreement",
        "transfer:describeConnector",
        "transfer:describeExecution",
        "transfer:describeProfile",
        "transfer:describeServer",
        "transfer:describeUser",
        "transfer:describeWebApp",
        "transfer:describeWebAppCustomization",
        "transfer:describeWorkflow",
        "transfer:listAccesses",
        "transfer:listAgreements",
        "transfer:listConnectors",
        "transfer:listExecutions",
        "transfer:listHostKeys",
        "transfer:listProfiles",
        "transfer:listServers",
        "transfer:listTagsForResource",
        "transfer:listUsers",
        "transfer:listWebApps",
        "transfer:listWorkflows",
        "transfer:sendWorkflowStepState",
        "trustedadvisor:getOrganizationRecommendation",
        "trustedadvisor:getRecommendation",
        "trustedadvisor:listChecks",
        "trustedadvisor:listOrganizationRecommendationAccounts",
```

```
        "trustedadvisor:listOrganizationRecommendationResources",
        "trustedadvisor:listOrganizationRecommendations",
        "trustedadvisor:listRecommendationResources",
        "trustedadvisor:listRecommendations",
        "verifiedpermissions:getIdentitySource",
        "verifiedpermissions:getPolicy",
        "verifiedpermissions:getPolicyStore",
        "verifiedpermissions:getPolicyTemplate",
        "verifiedpermissions:getSchema",
        "verifiedpermissions:listIdentitySources",
        "verifiedpermissions:listPolicies",
        "verifiedpermissions:listPolicyStores",
        "verifiedpermissions:listPolicyTemplates",
        "vpc-lattice:getAccessLogSubscription",
        "vpc-lattice:getAuthPolicy",
        "vpc-lattice:getDomainVerification",
        "vpc-lattice:getListener",
        "vpc-lattice:getResourceConfiguration",
        "vpc-lattice:getResourceGateway",
        "vpc-lattice:getResourcePolicy",
        "vpc-lattice:getRule",
        "vpc-lattice:getService",
        "vpc-lattice:getServiceNetwork",
        "vpc-lattice:getServiceNetworkResourceAssociation",
        "vpc-lattice:getServiceNetworkServiceAssociation",
        "vpc-lattice:getServiceNetworkVpcAssociation",
        "vpc-lattice:getTargetGroup",
        "vpc-lattice:listAccessLogSubscriptions",
        "vpc-lattice:listDomainVerifications",
        "vpc-lattice:listListeners",
        "vpc-lattice:listResourceConfigurations",
        "vpc-lattice:listResourceEndpointAssociations",
        "vpc-lattice:listResourceGateways",
        "vpc-lattice:listRules",
        "vpc-lattice:listServiceNetworks",
        "vpc-lattice:listServiceNetworkResourceAssociations",
        "vpc-lattice:listServiceNetworkServiceAssociations",
        "vpc-lattice:listServiceNetworkVpcAssociations",
        "vpc-lattice:listServiceNetworkVpcEndpointAssociations",
        "vpc-lattice:listServices",
        "vpc-lattice:listTargetGroups",
        "vpc-lattice:listTargets",
        "waf-regional:getByteMatchSet",
        "waf-regional:getChangeTokenStatus",
```

```
        "waf-regional:getGeoMatchSet",
        "waf-regional:getIPSet",
        "waf-regional:getLoggingConfiguration",
        "waf-regional:getRateBasedRule",
        "waf-regional:getRegexMatchSet",
        "waf-regional:getRegexPatternSet",
        "waf-regional:getRule",
        "waf-regional:getRuleGroup",
        "waf-regional:getSqlInjectionMatchSet",
        "waf-regional:getWebACL",
        "waf-regional:getWebACLForResource",
        "waf-regional:listActivatedRulesInRuleGroup",
        "waf-regional:listByteMatchSets",
        "waf-regional:listGeoMatchSets",
        "waf-regional:listIPSets",
        "waf-regional:listLoggingConfigurations",
        "waf-regional:listRateBasedRules",
        "waf-regional:listRegexMatchSets",
        "waf-regional:listRegexPatternSets",
        "waf-regional:listResourcesForWebACL",
        "waf-regional:listRuleGroups",
        "waf-regional:listRules",
        "waf-regional:listSqlInjectionMatchSets",
        "waf-regional:listWebACLs",
        "waf:getByteMatchSet",
        "waf:getChangeTokenStatus",
        "waf:getGeoMatchSet",
        "waf:getIPSet",
        "waf:getLoggingConfiguration",
        "waf:getRateBasedRule",
        "waf:getRegexMatchSet",
        "waf:getRegexPatternSet",
        "waf:getRule",
        "waf:getRuleGroup",
        "waf:getSampledRequests",
        "waf:getSizeConstraintSet",
        "waf:getSqlInjectionMatchSet",
        "waf:getWebACL",
        "waf:getXssMatchSet",
        "waf:listActivatedRulesInRuleGroup",
        "waf:listByteMatchSets",
        "waf:listGeoMatchSets",
        "waf:listIPSets",
        "waf:listLoggingConfigurations",
```

```
        "waf:listRateBasedRules",
        "waf:listRegexMatchSets",
        "waf:listRegexPatternSets",
        "waf:listRuleGroups",
        "waf:listRules",
        "waf:listSizeConstraintSets",
        "waf:listSqlInjectionMatchSets",
        "waf:listWebACLs",
        "waf:listXssMatchSets",
        "wafv2:checkCapacity",
        "wafv2:describeManagedRuleGroup",
        "wafv2:getIPSet",
        "wafv2:getLoggingConfiguration",
        "wafv2:getPermissionPolicy",
        "wafv2:getRateBasedStatementManagedKeys",
        "wafv2:getRegexPatternSet",
        "wafv2:getRuleGroup",
        "wafv2:getSampledRequests",
        "wafv2:getWebACL",
        "wafv2:getWebACLForResource",
        "wafv2:listAvailableManagedRuleGroups",
        "wafv2:listIPSets",
        "wafv2:listLoggingConfigurations",
        "wafv2:listRegexPatternSets",
        "wafv2:listResourcesForWebACL",
        "wafv2:listRuleGroups",
        "wafv2:listTagsForResource",
        "wafv2:listWebACLs",
        "workdocs:checkAlias",
        "workdocs:describeAvailableDirectories",
        "workdocs:describeInstances",
        "workmail:describeGroup",
        "workmail:describeOrganization",
        "workmail:describeResource",
        "workmail:describeUser",
        "workmail:listAliases",
        "workmail:listGroupMembers",
        "workmail:listGroups",
        "workmail:listMailboxPermissions",
        "workmail:listOrganizations",
        "workmail:listResourceDelegates",
        "workmail:listResources",
        "workmail:listUsers",
        "workspaces-web:getBrowserSettings",
```

```
        "workspaces-web:getIdentityProvider",
        "workspaces-web:getNetworkSettings",
        "workspaces-web:getPortal",
        "workspaces-web:getPortalServiceProviderMetadata",
        "workspaces-web:getTrustStoreCertificate",
        "workspaces-web:getUserSettings",
        "workspaces-web:listBrowserSettings",
        "workspaces-web:listIdentityProviders",
        "workspaces-web:listNetworkSettings",
        "workspaces-web:listPortals",
        "workspaces-web:listTagsForResource",
        "workspaces-web:listTrustStoreCertificates",
        "workspaces-web:listTrustStores",
        "workspaces-web:listUserSettings",
        "workspaces:describeAccount",
        "workspaces:describeAccountModifications",
        "workspaces:describeApplicationAssociations",
        "workspaces:describeCustomWorkspaceImageImport",
        "workspaces:describeIpGroups",
        "workspaces:describeTags",
        "workspaces:describeWorkspaceAssociations",
        "workspaces:describeWorkspaceBundles",
        "workspaces:describeWorkspaceDirectories",
        "workspaces:describeWorkspaceImages",
        "workspaces:describeWorkspaces",
        "workspaces:describeWorkspaceSnapshots",
        "workspaces:describeWorkspacesConnectionStatus",
        "workspaces:describeWorkspacesPools",
        "workspaces:describeWorkspacesPoolSessions",
        "xray:getEncryptionConfig",
        "xray:getGroup",
        "xray:getGroups",
        "xray:getInsightImpactGraph",
        "xray:getSamplingRules",
        "xray:getSamplingStatisticSummaries",
        "xray:getSamplingTargets",
        "xray:getServiceGraph",
        "xray:getTimeSeriesServiceStatistics",
        "xray:getTraceGraph",
        "xray:listResourcePolicies"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSystemsManagerAccountDiscoveryServicePolicy

Deskripsi: Mem AWS berikan izin Manajer Sistem (SSM) untuk menemukan Akun AWS informasi.

`AWSSystemsManagerAccountDiscoveryServicePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 24 Oktober 2019, 17:21 UTC
- Waktu teredit: 17 Oktober 2022, 20.25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSystemsManagerChangeManagementServicePolicy

Deskripsi: Menyediakan akses ke AWS sumber daya yang dikelola atau digunakan oleh kerangka kerja manajemen perubahan Manajer AWS Sistem.

`AWSSystemsManagerChangeManagementServicePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 07 Desember 2020, 22:21 UTC
- Waktu teredit: 23 Oktober 2025, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation",
        "ssm:CreateOpsItem",
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:GetAutomationExecution",
        "ssm:GetCalendarState",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:IsMemberInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetGroup",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSystemsManagerEnableConfigRecordingExecutionPolicy

Deskripsi: Memberikan izin untuk AWS Pengaturan Cepat Manajer Sistem untuk mengaktifkan dan meng AWS konfigurasi perekaman konfigurasi konfigurasi.

`AWSSystemsManagerEnableConfigRecordingExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSystemsManagerEnableConfigRecordingExecutionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juni 2024, 09:40 UTC
- Waktu teredit: 26 Juni 2024, 09:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerEnableConfigRecordingExecutionPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3BucketCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
```

```
        "s3:PutBucketPublicAccessBlock",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-quick-setup-config-recording-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SNSTopicsListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DefaultSNSTopicCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:ConfigRecording-Default-Topic"
    },
    {
      "Sid" : "ConfigureAndStartConfigurationRecorderPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeDeliveryChannels",
        "config:PutConfigurationRecorder",
        "config:PutDeliveryChannel",
        "config:StartConfigurationRecorder"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetAndPassConfigSLRPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
        "arn:aws:iam::*:role/AWSServiceRoleForConfig"
      ]
    },
    {
      "Sid" : "CreateConfigSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSystemsManagerEnableExplorerExecutionPolicy

Deskripsi: Kebijakan ini memberikan izin administratif untuk mengaktifkan Explorer, kemampuan Manajer AWS Sistem. Ini termasuk izin untuk memperbarui pengaturan layanan Manajer Sistem terkait, dan untuk membuat peran terkait layanan untuk Manajer Sistem.

`AWSSystemsManagerEnableExplorerExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSystemsManagerEnableExplorerExecutionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juni 2024, 09:42 UTC
- Waktu teredit: 26 Juni 2024, 09:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSystemsManagerForSAPFullAccess

Deskripsi: Menyediakan akses penuh ke AWS System Manager untuk layanan SAP

`AWSSystemsManagerForSAPFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSystemsManagerForSAPFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 November 2022, 02:11 UTC
- Waktu teredit: 10 Juli 2024, 21:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AwsSsmForSapPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    },
    {
      "Sid" : "AwsSsmForSapServiceRoleCreationPermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm-sap.amazonaws.com/
AWSServiceRoleForAWSSSMForSAP"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm-sap.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2StartStopPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "ec2:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSystemsManagerForSAPReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Manajer AWS Sistem untuk layanan SAP

`AWSSystemsManagerForSAPReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSystemsManagerForSAPReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 November 2022, 02:11 UTC
- Waktu teredit: 17 November 2022, 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:get*",
        "ssm-sap:list*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSystemsManagerJustInTimeAccessServicePolicy

Deskripsi: Menyediakan akses ke AWS sumber daya yang dikelola atau digunakan oleh Manajer AWS Sistem tepat waktu kerangka akses.

`AWSSystemsManagerJustInTimeAccessServicePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 21 April 2025, 20:07 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerJustInTimeAccessServicePolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOpsItemReplication",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:opsitem/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "Replica"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOpsItemReplicationTagging",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:opsitem/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "Replica"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAutomationExecutionTagging",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOpsItemManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:opsitem/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "AllowRetrieveDocument",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : [
            "ManualApprovalPolicy",
            "AutoApprovalPolicy"
          ]
        }
      }
    },
    {
      "Sid" : "AllowDescriptions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeOpsItems",
        "ssm:DescribeSessions",
        "ssm:ListDocuments"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowListTagsForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:managed-instance/*"
      ]
    },
```

```
    {
      "Sid" : "AllowListSSMGUIConnections",
      "Effect" : "Allow",
      "Action" : [
        "ssm-guiconnect:ListConnections"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowIdentityStoreActions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:DescribeUser",
        "identitystore:GetGroupId",
        "identitystore:GetUserId"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowSSODirectoryActions",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:IsMemberInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowSSOInstanceActions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "AllowDescribingEC2Tags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowPublishingCloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/SSM/JustInTimeAccess"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSystemsManagerJustInTimeAccessTokenPolicy

Deskripsi: Kebijakan terkelola AWSSystemsManagerJustInTimeAccessTokenPolicy memungkinkan Manajer Sistem menghasilkan token akses yang digunakan untuk akses node tepat waktu.

`AWSSystemsManagerJustInTimeAccessTokenPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSystemsManagerJustInTimeAccessTokenPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 April 2025, 21:07 UTC

- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeAccessTokenPolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SsmStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/SSM-SessionManagerRunShell"
      ]
    },
    {
      "Sid" : "TerminateAndResumeSessionAndOpenDataChannel",
      "Effect" : "Allow",
      "Action" : [
        "ssm:TerminateSession",
        "ssm:ResumeSession",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    },
    {
      "Sid" : "GuiConnect",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm-guiconnect:CancelConnection",
        "ssm-guiconnect:GetConnection",
        "ssm-guiconnect:StartConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SessionManagerKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RdpKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm-guiconnect.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "RdpStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/AWS-StartPortForwardingSession"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetup",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListDirectoryAssociations*",
        "identitystore:DescribeUser",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetupSendCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/AWSSSO-CreateSSOUser"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSystemsManagerJustInTimeAccessTokenSessionPolicy

Deskripsi: Kebijakan ter AWSSystemsManagerJustInTimeAccessTokenSessionPolicy kelola memungkinkan Manajer Sistem untuk menerapkan izin terbatasnya ke sesi akses node tepat waktu setelah dimulai.

`AWSSystemsManagerJustInTimeAccessTokenSessionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSystemsManagerJustInTimeAccessTokenSessionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 April 2025, 20:52 UTC
- Waktu teredit: 12 Februari 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeAccessTokenSessionPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SsmStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/SSM-SessionManagerRunShell"
      ]
    },
    {
      "Sid" : "GuiConnect",
      "Effect" : "Allow",
      "Action" : [
        "ssm-guiconnect:CancelConnection",
        "ssm-guiconnect:GetConnection",
        "ssm-guiconnect:StartConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SessionManagerKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "RdpKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm-guiconnect.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "RdpStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-StartPortForwardingSession"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetup",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListDirectoryAssociations*",
        "identitystore:DescribeUser",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetupSendCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSSSO-CreateSSOUser"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy

Deskripsi: Kebijakan ini memungkinkan Manajer Sistem membagikan kebijakan penolakan akses untuk akses node tepat waktu dari akun administrator yang didelegasikan ke akun anggota, dan mereplikasi kebijakan ke beberapa Wilayah.

`AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 April 2025, 20:52 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QuickSetupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-quicksetup:GetConfigurationManager",
        "cloudformation:ListStackSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QuickSetupOrganizationsPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "ssm-quicksetup.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "QuickSetupSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm-quicksetup.amazonaws.com/
AWSServiceRoleForSSMQuickSetup"
      ]
    },
    {
      "Sid" : "OrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMDocumentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:ListTagsForResource",
        "ssm:PutResourcePolicy",
        "ssm:DeleteResourcePolicy",
        "ssm:GetResourcePolicies"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SSM-JustInTimeAccessDenyAccessOrgPolicy",
      "Condition" : {
        "StringEquals" : {
```

```
          "ssm:DocumentType" : "AutoApprovalPolicy"
        }
      }
    },
    {
      "Sid" : "SSMDocumentCreateReplicaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SSM-JustInTimeAccessDenyAccessOrgPolicy",
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : "AutoApprovalPolicy",
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "SSMDocumentUpdateReplicaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateDocument",
        "ssm:UpdateDocumentDefaultVersion",
        "ssm:UpdateDocumentMetadata",
        "ssm:DeleteDocument",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SSM-JustInTimeAccessDenyAccessOrgPolicy",
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : "AutoApprovalPolicy",
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RAMReadPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        },
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "ssm:Document"
        },
        "ArnLikeIfExists" : {
          "ram:ResourceArn" : "arn:aws:ssm:*:*:document/SSM-
JustInTimeAccessDenyAccessOrgPolicy"
        }
      }
    },
    {
      "Sid" : "RAMTaggingPermissions",
      "Effect" : "Allow",
      "Action" : "ram:TagResource",
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "RAMModificationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:ResourceShareName" : "SSMJustInTimeNodeAccessManagedResourceShare",
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "ssm:Document"
        },
        "ArnLikeIfExists" : {
          "ram:ResourceArn" : "arn:aws:ssm:*:*:document/SSM-
JustInTimeAccessDenyAccessOrgPolicy"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSystemsManagerNotificationsServicePolicy

Deskripsi: Izin diperlukan untuk mengumpulkan informasi tentang pengguna untuk Just-In-Time-Node-Access pemberitahuan.

`AWSSystemsManagerNotificationsServicePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 17 April 2025, 20:52 UTC
- Waktu teredit: 17 April 2025, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerNotificationsServicePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowIdentityStoreActions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroupMemberships",
        "identitystore:DescribeUser"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "AllowSSOActions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowSSODirectoryActions",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUser",
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowIamActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSSystemsManagerOpsDataSyncServiceRolePolicy

Deskripsi: Peran IAM untuk SSM Explorer untuk mengelola operasi terkait OpsData

`AWSSystemsManagerOpsDataSyncServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 26 April 2021, 20:42 UTC
- Waktu teredit: 28 Juni 2023, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/ExplorerSecurityHubOpsItem" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "securityhub:GetFindings",
        "securityhub:BatchUpdateFindings"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "securityhub:ASFFSyntaxPath/Workflow.Status" : "SUPPRESSED"
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Confidence" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Criticality" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Note.Text" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Note.UpdatedBy" : false
        }
```

```
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/RelatedFindings" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Types" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/UserDefinedFields.key" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/UserDefinedFields.value" : false
        }
      }
    },
    {
      "Effect" : "Deny",
```

```
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/VerificationState" : false
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSThinkboxAssetServerPolicy

Deskripsi: Kebijakan ini memberikan izin yang diperlukan untuk operasi normal kepada Server Aset AWS Portal.

`AWSThinkboxAssetServerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSThinkboxAssetServerPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:18 UTC
- Waktu teredit: 27 Mei 2020, 19:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/thinkbox*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-portal-cache*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSThinkboxAWSPortalAdminPolicy

Deskripsi: Kebijakan ini memberikan perangkat lunak Tenggat Waktu AWS Thinkbox akses penuh ke beberapa AWS layanan seperti yang diperlukan untuk administrasi AWS Portal. Ini termasuk akses untuk membuat tag arbitrer pada beberapa jenis sumber daya EC2.

`AWSThinkboxAWSPortalAdminPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSThinkboxAWSPortalAdminPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:41 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxAWSPortal1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachInternetGateway",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
```

```
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreatePlacementGroup",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAddresses",
        "ec2:DescribeFleets",
        "ec2:DescribeFleetHistory",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNatGateways",
        "ec2:DescribeTags",
        "ec2:DescribeKeyPairs",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRegions",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:GetConsoleOutput",
        "ec2:ImportKeyPair",
        "ec2:ReleaseAddress",
        "ec2:RequestSpotFleet",
        "ec2:CancelSpotFleetRequests",
        "ec2:DisassociateAddress",
        "ec2:DeleteFleets",
```

```
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteVpc",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DisassociateRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DeleteNatGateway",
        "ec2:DetachInternetGateway",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyFleet",
        "ec2:ModifySpotFleetRequest",
        "ec2:ModifyVpcAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal2",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal3",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/AWSPortal*"
```

```
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal4",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/aws:cloudformation:logical-id" : "ReverseForwarder"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal5",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : false
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal6",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:PlacementGroup" : "arn:aws:ec2:*:*:placement-group/
*DeadlinePlacementGroup*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
```

```
      "Condition" : {
        "ArnLike" : {
          "ec2:PlacementGroup" : "arn:aws:ec2:*:*:placement-group/
*DeadlinePlacementGroup*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal10",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal11",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AWSPortal*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal12",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:ListEntitiesForPolicy",
        "iam:ListPolicyVersions"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/AWSPortal*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal13",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPortal*",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal14",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/AWSPortal*",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2fleet.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal15",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ec2fleet.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal16",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:PutBucketAcl",
        "s3:PutBucketCORS",
        "s3:PutBucketVersioning",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:PutBucketLogging",
```

```
        "s3:PutBucketTagging",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObjectVersion"
      ],
      "Resource" : [
        "arn:aws:s3::*:awsportal*",
        "arn:aws:s3::*:stack*",
        "arn:aws:s3::*:aws-portal-cache*",
        "arn:aws:s3::*:logs-for-aws-portal-cache*",
        "arn:aws:s3::*:logs-for-stack*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal17",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3::*:logs-for-aws-portal-cache*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal18",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketOwnershipControls"
      ],
      "Resource" : [
        "arn:aws:s3::*:logs-for-stack*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal19",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal20",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal21",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListStackResources",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/stack*/*",
        "arn:aws:cloudformation:*:*:stack/Deadline*/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal22",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:EstimateTemplateCost",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AWSThinkboxAWSPortal23",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:PutRetentionPolicy",
        "logs:DeleteRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/thinkbox*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal24",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal25",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal26",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : [
            "rcs-tls-pw*"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal27",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSThinkboxAWSPortalGatewayPolicy

Deskripsi: Kebijakan ini memberi mesin AWS Portal Gateway izin yang diperlukan untuk operasi normal.

`AWSThinkboxAWSPortalGatewayPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSThinkboxAWSPortalGatewayPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:05 UTC
- Waktu teredit: 30 Juni 2020, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/thinkbox*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-portal-cache*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "dynamodb:Scan",
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::stack*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::stack*/gateway_certs/*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw-stack*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSThinkboxAWSPortalWorkerPolicy

Deskripsi: Kebijakan ini memberikan izin yang diperlukan untuk operasi normal kepada Pekerja Tenggat Waktu di AWS Portal.

`AWSThinkboxAWSPortalWorkerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSThinkboxAWSPortalWorkerPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:15 UTC
- Waktu teredit: 07 Desember 2020, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/DeadlineRole" : "DeadlineRenderNode"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::aws-portal-cache*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::stack*/gateway_certs/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/thinkbox*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWS*"
      ]
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSThinkboxDeadlineResourceTrackerAccessPolicy

Deskripsi: Memberikan izin yang diperlukan untuk pengoperasian Pelacak AWS Sumber Daya Tenggat Waktu Thinkbox. Ini termasuk akses penuh ke beberapa tindakan EC2, termasuk DeleteFleets dan CancelSpotFleetRequests.

`AWSThinkboxDeadlineResourceTrackerAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSThinkboxDeadlineResourceTrackerAccessPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:25 UTC
- Waktu teredit: 27 Mei 2020, 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAccessPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListStreams"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchWriteItem",
        "dynamodb:DeleteItem",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:PutItem",
        "dynamodb:Scan",
        "dynamodb:UpdateItem",
        "dynamodb:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeHealth*",
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeInfo*",
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelSpotFleetRequests",
```

```
        "ec2:DeleteFleets",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeFleets",
        "ec2:DescribeInstances",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/DeadlineTrackedAWSResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutEvents"
      ],
      "Resource" : [
        "arn:aws:events:*:*:event-bus/default"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/DeadlineResourceTracker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:ReceiveMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeStateMessageQueue*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSThinkboxDeadlineResourceTrackerAdminPolicy

Deskripsi: Memberikan izin yang diperlukan untuk membuat, menghancurkan, dan mengelola Pelacak AWS Sumber Daya Tenggat Waktu Thinkbox.

`AWSThinkboxDeadlineResourceTrackerAdminPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSThinkboxDeadlineResourceTrackerAdminPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:29 UTC
- Waktu teredit: 16 Juli 2026, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAdminPolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker1",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
```

```
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker2",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker3",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DeadlineResourceTracker*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker4",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable",
        "dynamodb:ListTagsOfResource",
        "dynamodb:TagResource",
```

```
        "dynamodb:UntagResource"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeHealth*",
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeInfo*",
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker5",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchWriteItem",
        "dynamodb:Scan"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker6",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/DeadlineResourceTracker*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker7",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DeadlineResourceTracker*"
      ]
    },
```

```
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker8",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker9",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker10",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DeadlineResourceTrackerAccess*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker11",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/dynamodb.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_DynamoDBTable"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker12",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetEventSourceMapping"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker13",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateEventSourceMapping",
        "lambda:DeleteEventSourceMapping"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnLike" : {
          "lambda:FunctionArn" : [
            "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker14",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ],
      "Condition" : {
        "StringLike" : {
          "lambda:Principal" : "events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker15",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:DeleteFunctionConcurrency",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "lambda:PutFunctionConcurrency",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker16",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::*/deadline_aws_resource_tracker*.zip",
        "arn:aws:s3:::*/DeadlineAWSResourceTrackerTemplate*.yaml"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker17",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:TagQueue",
        "sqs:UntagQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*",
        "arn:aws:sqs:*:*:DeadlineResourceTracker*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

Deskripsi: Memberikan izin yang diperlukan untuk Plugin Acara Spot Tenggat Waktu AWS Thinkbox. Ini termasuk izin untuk meminta, memodifikasi, dan membatalkan armada spot, serta PassRole izin terbatas.

`AWSThinkboxDeadlineSpotEventPluginAdminPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSThinkboxDeadlineSpotEventPluginAdminPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:38 UTC
- Waktu teredit: 27 Mei 2020, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginAdminPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelSpotFleetRequests",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "ec2:RequestSpotFleet"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role",
```

```
        "arn:aws:iam::*:role/DeadlineSpot*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

Deskripsi: Memberikan izin yang diperlukan untuk instans EC2 yang menjalankan perangkat lunak AWS Thinkbox Deadline Spot Event Plugin Worker.

`AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSThinkboxDeadlineSpotEventPluginWorkerPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:35 UTC
- Waktu teredit: 07 Desember 2020, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeTags"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/DeadlineTrackedAWSResource" : "SpotEventPlugin"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/DeadlineResourceTracker" : "SpotEventPlugin"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueUrl",
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSTransferConsoleFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Transfer melalui Konsol Manajemen AWS

`AWSTransferConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTransferConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Desember 2020, 19:33 UTC
- Waktu teredit: 14 Desember 2020, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "transfer.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
```

```
        "ec2:DescribeVpcEndpoints",
        "health:DescribeEventAggregates",
        "iam:GetPolicyVersion",
        "iam:ListPolicies",
        "iam:ListRoles",
        "route53:ListHostedZones",
        "s3:ListAllMyBuckets",
        "transfer:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSTransferFullAccess

Deskripsi: Menyediakan akses penuh ke Layanan AWS Transfer.

`AWSTransferFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTransferFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Desember 2020, 19:37 UTC
- Waktu teredit: 14 Desember 2020, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "transfer:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "transfer.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSTransferLoggingAccess

Deskripsi: AWS Memungkinkan Transfer akses penuh untuk membuat aliran log dan grup dan menempatkan peristiwa log ke akun Anda

`AWSTransferLoggingAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTransferLoggingAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Januari 2019, 15:32 UTC
- Waktu teredit: 14 Januari 2019, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSTransferReadOnlyAccess

Deskripsi: Menyediakan akses readonly ke layanan AWS Transfer.

`AWSTransferReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTransferReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Agustus 2020, 17:54 UTC
- Waktu teredit: 27 Agustus 2020, 17:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSTransferServiceRolePolicy

Deskripsi: Mengizinkan Transfer untuk berintegrasi dengan AWS layanan lain atas nama Anda

`AWSTransferServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 22 September 2026, 17:07 UTC
- Waktu teredit: 22 September 2026, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTransferServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TransferSecretsManagerBatchAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:BatchGetSecretValue",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "TransferSecretsManagerReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:transfer!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "transfer",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TransferSecretsManagerDeleteAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:transfer!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "transfer",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Bool" : {
          "secretsmanager:ForceDeleteWithoutRecovery" : false
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSTransformApplicationDeploymentPolicy

Deskripsi: Mengaktifkan layanan AWS Transform untuk menerapkan aplikasi.NET yang diubah dengan membuat dan mengelola AWS sumber daya. Kebijakan ini memberikan izin untuk menyediakan infrastruktur, mengelola sumber daya komputasi, dan mengonfigurasi setelan penerapan di berbagai AWS layanan.

`AWSTransformApplicationDeploymentPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTransformApplicationDeploymentPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 28 Agustus 2025, 06:34 UTC
- Waktu teredit: 11 September 2026, 00:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransformApplicationDeploymentPolicy`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/AWSTransform*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*"
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
```

```
          "cloudformation:CreateAction" : [
            "CreateStack",
            "UpdateStack"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInternetGateways"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ForAnyValue:StringNotEquals" : {
          "aws:TagKeys" : [
            "Name",
            "CreatedBy",
            "ApplicationName",
            "TransformationType",
            "aws:cloudformation:stack-name",
            "aws:cloudformation:logical-id",
            "aws:cloudformation:stack-id"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
```

```
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        }
      },
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-Builder-Instance-Role",
        "arn:aws:iam::*:instance-profile/AWSTransform-Deploy-Builder-Instance-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-App-Instance-Role",
        "arn:aws:iam::*:instance-profile/AWSTransform-Deploy-App-Instance-Role"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-Builder-Instance-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-App-Instance-Role"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/ami-amazon-linux-latest*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:ModifyInstanceAttribute"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunRemoteScript"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:PutObject",
        "s3:ListMultipartUploadParts",
```

```
        "s3:ListBucketMultipartUploads",
        "s3:AbortMultipartUpload",
        "s3:PutBucketTagging"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-transform-deployment-bucket-*",
        "arn:aws:s3:::aws-transform-deployment-bucket-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedFor" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws-transform" : "*",
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ],
          "kms:EncryptionContext:aws:ebs:id" : "*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "kms:GrantConstraintType" : "EncryptionContextSubset"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
```

```
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSTransformApplicationECSDeploymentPolicy

Deskripsi: Mengaktifkan AWS Transform untuk menyebarkan aplikasi ke Amazon Elastic Container Service (ECS) dengan Fargate. Ini memberikan izin untuk menyediakan, mengkonfigurasi, dan mengelola infrastruktur dasar yang diperlukan untuk menjalankan aplikasi di ECS.

`AWSTransformApplicationECSDeploymentPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTransformApplicationECSDeploymentPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 29 September 2025, 22:49 UTC
- Waktu teredit: 11 September 2026, 00:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransformApplicationECSDeploymentPolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:CreateStack",
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
```

```
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack",
            "UpdateStack"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:CreateCluster",
      "Resource" : "arn:aws:ecs:*:*:cluster/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateCluster",
        "ecs:DeleteCluster"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/AWSTransform*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ecs:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:RegisterTaskDefinition",
      "Resource" : "arn:aws:ecs:*:*:task-definition/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:RunTask",
      "Resource" : "arn:aws:ecs:*:*:task-definition/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        },
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/AWSTransform*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:ListTasks",
      "Resource" : "arn:aws:ecs:*:*:container-instance/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/AWSTransform*"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "ecs:DescribeTasks",
      "Resource" : "arn:aws:ecs:*:*:task/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/AWSTransform*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Task-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Execution-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "ecs-tasks.amazonaws.com",
            "ecs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Task-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Execution-Role"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:CreateService",
      "Resource" : "arn:aws:ecs:*:*:service/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:DeleteService"
      ],
      "Resource" : "arn:aws:ecs:*:*:service/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ecs:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/AWSTransform*",
        "arn:aws:ecs:*:*:task-definition/AWSTransform*",
        "arn:aws:ecs:*:*:service/AWSTransform*",
        "arn:aws:ecs:*:*:task/AWSTransform*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "logs:UntagResource",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:GetLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*:log-stream:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/awstransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
```

```
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ecr.*.amazonaws.com"
          ],
```

```
          "kms:EncryptionContext:aws:ecr:arn" : "*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "kms:GrantConstraintType" : "EncryptionContextSubset"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "GenerateDataKey"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSTransformCustomExecuteTransformations

Deskripsi: Menyediakan akses untuk menjalankan transformasi di AWS Transform kustom.

`AWSTransformCustomExecuteTransformations`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTransformCustomExecuteTransformations` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Desember 2025, 15:34 UTC

- Waktu teredit: 27 April 2026, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformCustomExecuteTransformations`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSTransformCustomExecuteTransformations",
      "Effect" : "Allow",
      "Action" : [
        "transform-custom:ConverseStream",
        "transform-custom:ExecuteTransformation",
        "transform-custom:GetCampaign",
        "transform-custom:UpdateCampaignRepositoryStatus",
        "transform-custom:UpdateCampaign"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/transform-custom.amazonaws.com/
AWSServiceRoleForAWSTransformCustom"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:AWSServiceName" : "transform-custom.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSTransformCustomFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Transform kustom.

`AWSTransformCustomFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTransformCustomFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Desember 2025, 15:19 UTC
- Waktu teredit: 07 April 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformCustomFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSTransformCustomAllActions",
      "Effect" : "Allow",
      "Action" : [
        "transform-custom:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/transform-custom.amazonaws.com/
AWSServiceRoleForAWSTransformCustom"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "transform-custom.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSTransformCustomManageTransformations

Deskripsi: Memungkinkan pengelolaan sumber daya transformasi dan pelaksanaan transformasi di kustom AWS Transform.

`AWSTransformCustomManageTransformations`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTransformCustomManageTransformations` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Desember 2025, 15:49 UTC
- Waktu teredit: 27 April 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformCustomManageTransformations`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSTransformCustomManageTransformations",
      "Effect" : "Allow",
      "Action" : [
        "transform-custom:ConverseStream",
        "transform-custom:CreateTransformationPackageUrl",
        "transform-custom:CompleteTransformationPackageUpload",
```

```
        "transform-custom:DeleteTransformationPackage",
        "transform-custom:GetTransformationPackageUrl",
        "transform-custom:ListTransformationPackageMetadata",
        "transform-custom:ExecuteTransformation",
        "transform-custom:ListKnowledgeItems",
        "transform-custom:GetKnowledgeItem",
        "transform-custom:DeleteKnowledgeItem",
        "transform-custom:UpdateKnowledgeItemConfiguration",
        "transform-custom:UpdateKnowledgeItemStatus",
        "transform-custom:GetCampaign",
        "transform-custom:UpdateCampaignRepositoryStatus",
        "transform-custom:UpdateCampaign",
        "transform-custom:ListTagsForResource",
        "transform-custom:TagResource",
        "transform-custom:UntagResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/transform-custom.amazonaws.com/
AWSServiceRoleForAWSTransformCustom"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "transform-custom.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSTransformInfrastructureExecutorAccessBatch

Deskripsi: Memberikan peran eksekusi pengembang izin yang diperlukan untuk menjalankan AWS Transform Continuous Modernization CLI/agent untuk dijalankan assessments/transformations menggunakan AWS Batch, termasuk mengunggah kode sumber, mengambil hasil, memantau status pekerjaan Batch, membaca log, dan mengelola jadwal transformasi.

`AWSTransformInfrastructureExecutorAccessBatch`hadalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTransformInfrastructureExecutorAccessBatch` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 Juli 2026, 20:12 UTC
- Waktu teredit: 02 September 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformInfrastructureExecutorAccessBatch`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "LambdaInvokeATXFunctions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:GetFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:atx-trigger-job-*",
        "arn:aws:lambda:*:*:function:atx-trigger-batch-jobs-*",
        "arn:aws:lambda:*:*:function:atx-get-job-status-*",
        "arn:aws:lambda:*:*:function:atx-get-batch-status-*",
        "arn:aws:lambda:*:*:function:atx-list-jobs-*",
        "arn:aws:lambda:*:*:function:atx-list-batches-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3UploadSourceCode",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::atx-source-code-*",
        "arn:aws:s3:::atx-source-code-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3DownloadResults",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::atx-custom-output-*",
        "arn:aws:s3:::atx-custom-output-*/*",
        "arn:aws:s3:::atx-ct-output-*",
        "arn:aws:s3:::atx-ct-output-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3WriteBatchSidecar",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::atx-custom-output-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSEncryptDecrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
```

```
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : [
            "alias/atx-encryption-key",
            "alias/atx-encryption-key-*"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchReadLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/batch/atx-transform*",
        "arn:aws:logs:*:*:log-group:/aws/batch/job*",
        "arn:aws:logs:*:*:log-group:AtxVpc*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/atx-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchDashboard",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetDashboard",
        "cloudwatch:ListDashboards"
      ],
      "Resource" : [
        "arn:aws:cloudwatch::*:dashboard/ATX-Transform-CLI-Dashboard",
        "arn:aws:cloudwatch::*:dashboard/ATX-Transform-CLI-Dashboard-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "BatchDescribe",
      "Effect" : "Allow",
      "Action" : [
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeJobDefinitions",
        "batch:DescribeJobs",
        "batch:ListJobs"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CheckInfrastructureStatus",
      "Effect" : "Allow",
      "Action" : "cloudformation:DescribeStacks",
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/AtxInfrastructureStack/*",
        "arn:aws:cloudformation:*:*:stack/AtxInfrastructureStack-*/*",
        "arn:aws:cloudformation:*:*:stack/atx-*",
        "arn:aws:cloudformation:*:*:stack/atx-*/*",
        "arn:aws:cloudformation:*:*:stack/AtxSecurityAgentStack-*/*",
        "arn:aws:cloudformation:*:*:stack/AtxDispatcherStack/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerATXSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:atx/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SchedulerManage",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:CreateSchedule",
        "scheduler:DeleteSchedule",
        "scheduler:GetSchedule",
        "scheduler:UpdateSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListSchedules"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule-group/atx-ct",
        "arn:aws:scheduler:*:*:schedule-group/atx-ct-*",
        "arn:aws:scheduler:*:*:schedule/atx-ct/*",
        "arn:aws:scheduler:*:*:schedule/atx-ct-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PassSchedulerRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AtxSchedulerInvocationRole",
        "arn:aws:iam::*:role/AtxSchedulerInvocationRole-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "scheduler.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "EC2NetworkDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNatGateways"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMReadRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:GetRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/ATX*",
        "arn:aws:iam::*:role/Atx*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagGetATXStacks",
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "CFNListStacksForDetect",
      "Effect" : "Allow",
      "Action" : "cloudformation:ListStacks",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SQSEnqueueToDispatcher",
      "Effect" : "Allow",
      "Action" : "sqs:SendMessage",
      "Resource" : "arn:aws:sqs:*:*:atx-dispatcher-queue",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSTransformInfrastructureExecutorAccessEC2

Deskripsi: Memberikan peran eksekusi pengembang izin yang diperlukan untuk menjalankan AWS Transform Continuous Modernization CLI/agent agar dijalankan assessments/transformations menggunakan EC2, termasuk mengunggah kode sumber, mengambil hasil, memantau status pekerjaan, membaca log, dan mengelola jadwal transformasi.

`AWSTransformInfrastructureExecutorAccessEC2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTransformInfrastructureExecutorAccessEC2` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 Juli 2026, 20:12 UTC
- Waktu teredit: 02 September 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformInfrastructureExecutorAccessEC2`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CFNRead",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStackDriftDetectionStatus"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/atx-*/*",
        "arn:aws:cloudformation:*:*:stack/AtxSecurityAgentStack-*/*",
        "arn:aws:cloudformation:*:*:stack/AtxDispatcherStack/*"
```

```
      ]
    },
    {
      "Sid" : "CFNValidateTemplate",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Desc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNatGateways",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2PowerState",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/atx-remote-infra" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "SSMRead",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:ListCommands",
        "ssm:ListCommandInvocations",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeSessions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SSMTgt",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/atx-remote-infra" : "true"
        }
      }
    },
    {
      "Sid" : "SSMDocs",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ssm:*::document/AWS-RunShellScript"
    },
    {
      "Sid" : "S3Data",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::atx-source-code-*",
        "arn:aws:s3:::atx-source-code-*/*",
        "arn:aws:s3:::atx-ct-output-*",
        "arn:aws:s3:::atx-ct-output-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSEncryptDecrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : [
            "alias/atx-encryption-key",
            "alias/atx-encryption-key-*"
          ]
        }
      }
    },
    {
      "Sid" : "SM",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:atx/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SMList",
      "Effect" : "Allow",
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SchedLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:CreateSchedule",
        "scheduler:DeleteSchedule",
        "scheduler:GetSchedule",
        "scheduler:UpdateSchedule"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule/atx-ct/*",
        "arn:aws:scheduler:*:*:schedule/atx-ct-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SchedGroupRead",
      "Effect" : "Allow",
      "Action" : "scheduler:GetScheduleGroup",
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule-group/atx-ct",
        "arn:aws:scheduler:*:*:schedule-group/atx-ct-*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SchedList",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassEC2InstanceRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/atx-transform-role",
        "arn:aws:iam::*:role/atx-transform-role-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassSchedulerRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AtxSchedulerInvocationRole",
        "arn:aws:iam::*:role/AtxSchedulerInvocationRole-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "scheduler.amazonaws.com",
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMReadRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/atx-*",
        "arn:aws:iam::*:role/Atx*",
        "arn:aws:iam::*:role/ATX*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMReadInstanceProfile",
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : [
        "arn:aws:iam::*:instance-profile/atx-*",
        "arn:aws:iam::*:instance-profile/Atx*",
        "arn:aws:iam::*:instance-profile/ATX*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagGetATXStacks",
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CFNListStacksForDetect",
      "Effect" : "Allow",
      "Action" : "cloudformation:ListStacks",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SQSEnqueueToDispatcher",
      "Effect" : "Allow",
      "Action" : "sqs:SendMessage",
      "Resource" : "arn:aws:sqs:*:*:atx-dispatcher-queue",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSTransformLandingZoneAgentPolicy

Deskripsi: Memberikan izin untuk AWS Transform untuk menyiapkan zona AWS pendaratan termasuk penyediaan akun, tata kelola organisasi, dan konfigurasi Menara Kontrol

`AWSTransformLandingZoneAgentPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTransformLandingZoneAgentPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Agustus 2026, 15:12 UTC
- Waktu teredit: 01 September 2026, 10:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformLandingZoneAgentPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3LandingZoneBucketAndObjectOperations",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:DeleteObject",
        "s3:GetBucketLocation",
```

```
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetObject",
        "s3:GetObjectAttributes",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:PutBucketPolicy",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::transform-vmware-landing-zone-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnLandingZoneStackCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:TagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AtxLz*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnLandingZoneStackUpdate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AtxLz*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnLandingZoneStackOperationsAndChangeSets",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplate",
        "cloudformation:ListChangeSets"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AtxLz*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ControlTowerAndOrganizationsOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "controltower:GetBaselineOperation",
        "controltower:GetControlOperation",
        "controltower:ListBaselines",
        "controltower:ListEnabledBaselines",
        "controltower:ListEnabledControls",
        "controltower:ListLandingZones",
        "organizations:DescribeCreateAccountStatus",
        "organizations:DescribeOrganization",
        "organizations:ListPolicies",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "ControlTowerResourceOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "controltower:GetEnabledBaseline",
        "controltower:GetEnabledControl",
        "controltower:GetLandingZone",
        "controltower:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:controltower:*:*:enabledbaseline/*",
        "arn:aws:controltower:*:*:enabledcontrol/*",
        "arn:aws:controltower:*:*:landingzone/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ControlTowerBaselineOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "controltower:GetBaseline"
      ],
      "Resource" : "arn:aws:controltower:*::baseline/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "ControlTowerEnableControlWithRequestTag",
      "Effect" : "Allow",
      "Action" : [
        "controltower:EnableControl"
      ],
      "Resource" : "arn:aws:controltower:*:*:enabledcontrol/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ControlTowerEnableBaselineAndOrganizationsAccountCreate",
      "Effect" : "Allow",
      "Action" : [
        "controltower:EnableBaseline",
        "controltower:TagResource",
        "organizations:CreateAccount"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "OrganizationsTagAndCreateOrganizationalUnit",
      "Effect" : "Allow",
      "Action" : [
        "organizations:CreateOrganizationalUnit",
        "organizations:TagResource"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/o-*/*",
        "arn:aws:organizations::*:ou/o-*/*",
        "arn:aws:organizations::*:policy/o-*/*",
        "arn:aws:organizations::*:root/o-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "OrganizationsResourceDescribeReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/*",
        "arn:aws:organizations::*:ou/*",
        "arn:aws:organizations::*:policy/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "OrganizationsPolicyUpdateViaControlTower",
      "Effect" : "Allow",
      "Action" : [
        "organizations:UpdatePolicy"
      ],
      "Resource" : "arn:aws:organizations::*:policy/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "controltower.amazonaws.com"
        },
        "StringEquals" : {
          "organizations:PolicyType" : "SERVICE_CONTROL_POLICY",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "OrganizationsHierarchyOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents"
      ],
```

```
      "Resource" : [
        "arn:aws:organizations::*:account/*",
        "arn:aws:organizations::*:ou/*",
        "arn:aws:organizations::*:root/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "OrganizationsMoveAccountWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "organizations:MoveAccount"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/*",
        "arn:aws:organizations::*:ou/*",
        "arn:aws:organizations::*:root/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "OrganizationsListTagsForResource",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/o-*/*",
        "arn:aws:organizations::*:ou/o-*/*",
        "arn:aws:organizations::*:policy/o-*/*",
        "arn:aws:organizations::*:root/o-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "OrganizationsServiceControlPolicyCreateViaControlTower",
      "Effect" : "Allow",
      "Action" : [
        "organizations:CreatePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "controltower.amazonaws.com"
        },
        "StringEquals" : {
          "organizations:PolicyType" : "SERVICE_CONTROL_POLICY"
        }
      }
    },
    {
      "Sid" : "OrganizationsServiceControlPolicyAttachViaControlTower",
      "Effect" : "Allow",
      "Action" : [
        "organizations:AttachPolicy"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/o-*/*",
        "arn:aws:organizations::*:ou/o-*/*",
        "arn:aws:organizations::*:policy/o-*/*",
        "arn:aws:organizations::*:root/o-*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "controltower.amazonaws.com"
        },
        "StringEquals" : {
          "organizations:PolicyType" : "SERVICE_CONTROL_POLICY",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ServiceCatalogProvisioningArtifactOperations",
```

```
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:CreateProvisioningArtifact",
        "servicecatalog:DeleteProvisioningArtifact",
        "servicecatalog:ListProvisioningArtifacts",
        "servicecatalog:UpdateProvisioningArtifact"
      ],
      "Resource" : "arn:aws:catalog:*:*:product/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSTransformNetworkMigrationAgentPolicy

Deskripsi: Memberikan izin untuk AWS Transform untuk menyebarkan dan mengonfigurasi infrastruktur jaringan termasuk VPC, Gerbang Transit, dan tabel rute untuk migrasi jaringan

`AWSTransformNetworkMigrationAgentPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTransformNetworkMigrationAgentPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 06 Agustus 2026, 15:27 UTC
- Waktu teredit: 01 September 2026, 10:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformNetworkMigrationAgentPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CfnNetworkMigrationStackCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnNetworkMigrationStackDescribeStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnNetworkMigrationStackListStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "CfnNetworkMigrationStackOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ListStackResources",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateTerminationProtection"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "Ec2NetworkProvisionCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
```

```
        "ec2:CreateInternetGateway",
        "ec2:CreateTransitGateway",
        "ec2:CreateVpc"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "Ec2NetworkTopologyOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:GetSubnetCidrReservations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "Ec2TagOnCreateNetworkMigration",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:network-insights-access-scope-analysis/*",
        "arn:aws:ec2:*:*:network-insights-access-scope/*",
        "arn:aws:ec2:*:*:network-insights-analysis/*",
```

```
        "arn:aws:ec2:*:*:network-insights-path/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:security-group-rule/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:transit-gateway-connect-peer/*",
        "arn:aws:ec2:*:*:transit-gateway-policy-table/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ec2:CreateAction" : [
            "AllocateAddress",
            "CreateInternetGateway",
            "CreateNatGateway",
            "CreateNetworkInsightsAccessScope",
            "CreateNetworkInsightsPath",
            "CreateNetworkInterface",
            "CreateRouteTable",
            "CreateSecurityGroup",
            "CreateSubnet",
            "CreateTransitGateway",
            "CreateTransitGatewayConnect",
            "CreateTransitGatewayConnectPeer",
            "CreateTransitGatewayPeeringAttachment",
            "CreateTransitGatewayPolicyTable",
            "CreateTransitGatewayPrefixListReference",
            "CreateTransitGatewayRoute",
            "CreateTransitGatewayRouteTable",
            "CreateTransitGatewayRouteTableAnnouncement",
            "CreateTransitGatewayVpcAttachment",
            "CreateVpc",
            "StartNetworkInsightsAnalysis"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "Ec2ViaCfnCrossOrgTgwAttachmentCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        }
      }
    },
    {
      "Sid" : "Ec2ViaCfnNetworkOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptTransitGatewayVpcAttachment",
        "ec2:AssociateNatGatewayAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateTransitGatewayRouteTable",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkInsightsAnalysis",
        "ec2:DeleteNetworkInsightsPath",
        "ec2:DeleteNetworkInterface",
```

```
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteTransitGateway",
        "ec2:DeleteTransitGatewayRoute",
        "ec2:DeleteTransitGatewayRouteTable",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:DeleteVpc",
        "ec2:DetachInternetGateway",
        "ec2:DisableTransitGatewayRouteTablePropagation",
        "ec2:DisassociateNatGatewayAddress",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyTransitGateway",
        "ec2:ModifyTransitGatewayVpcAttachment",
        "ec2:ModifyVpcAttribute",
        "ec2:RejectTransitGatewayVpcAttachment",
        "ec2:ReleaseAddress",
        "ec2:ReplaceRoute",
        "ec2:ReplaceTransitGatewayRoute",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAnalysis"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "Ec2ViaCfnNetworkProvisionCreateWithRequestTag",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInsightsPath",
        "ec2:CreateNetworkInterface",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "Ec2ViaCfnNetworkProvisionCreateWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInsightsPath",
        "ec2:CreateNetworkInterface",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
```

```
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "ec2:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "Ec2ViaCfnOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "Ec2ViaCfnSecurityGroupCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "Ec2ViaCfnSecurityGroupTagCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group-rule/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IamTgwServiceLinkedRoleCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/transitgateway.amazonaws.com/
AWSServiceRoleForVPCTransitGateway",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "iam:AWSServiceName" : "transitgateway.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IamViaCfnTgwLambdaRoleCleanupOperations",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
```

```
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "IamViaCfnTgwLambdaRoleCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IamViaCfnTgwLambdaRoleOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "IamViaCfnTgwLambdaRolePassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IamViaCfnTgwLambdaRolePolicyAttach",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/
AWSApplicationMigrationNetworkMigrationCustomResource",
            "arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
```

```
    },
    {
      "Sid" : "IamViaCfnTgwLambdaRoleTag",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "KmsS3EncryptionOperationsNetworkMigration",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/EncryptionKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LambdaViaCfnNetworkMigrationFunctionCreate",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:network-migration*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaViaCfnNetworkMigrationFunctionOperations",
      "Effect" : "Allow",
      "Action" : [
        "lambda:DeleteFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:network-migration*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "LambdaViaCfnNetworkMigrationFunctionReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:ListTags"
      ],
```

```
      "Resource" : "arn:aws:lambda:*:*:function:network-migration*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaViaCfnNetworkMigrationFunctionTag",
      "Effect" : "Allow",
      "Action" : [
        "lambda:TagResource"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:network-migration*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "LogsViaCfnNetworkMigrationOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/network-migration*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MgnNetworkMigrationDefinitionCreate",
      "Effect" : "Allow",
      "Action" : [
        "mgn:CreateNetworkMigrationDefinition"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "MgnNetworkMigrationDefinitionDelete",
      "Effect" : "Allow",
      "Action" : [
        "mgn:DeleteNetworkMigrationDefinition"
      ],
      "Resource" : "arn:aws:mgn:*:*:network-migration-definition/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : [
            "AWSTransform",
            "QTransform"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "MgnNetworkMigrationDefinitionOperations",
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetNetworkMigrationDefinition",
        "mgn:ListNetworkMigrationMappingUpdates",
        "mgn:StartNetworkMigrationMappingUpdate",
        "mgn:UpdateNetworkMigrationDefinition",
        "mgn:UpdateNetworkMigrationMapperSegment",
        "mgn:UpdateNetworkMigrationMapperSegmentConstruct"
      ],
      "Resource" : "arn:aws:mgn:*:*:network-migration-definition/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "MgnNetworkMigrationDefinitionTagOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "mgn:TagResource"
      ],
      "Resource" : "arn:aws:mgn:*:*:network-migration-definition/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "mgn:CreateAction" : "CreateNetworkMigrationDefinition"
        }
      }
    },
    {
      "Sid" : "NetworkMigrationOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "mgn:ListNetworkMigrationAnalyses",
```

```
        "mgn:ListNetworkMigrationAnalysisResults",
        "mgn:ListNetworkMigrationCodeGenerationSegments",
        "mgn:ListNetworkMigrationCodeGenerations",
        "mgn:ListNetworkMigrationDefinitions",
        "mgn:ListNetworkMigrationDeployedStacks",
        "mgn:ListNetworkMigrationDeployedStacksDeletions",
        "mgn:ListNetworkMigrationDeployments",
        "mgn:ListNetworkMigrationExecutions",
        "mgn:ListNetworkMigrationMapperSegmentConstructs",
        "mgn:ListNetworkMigrationMapperSegments",
        "mgn:ListNetworkMigrationExecutionArtifacts",
        "mgn:ListNetworkMigrationMappings"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "NetworkMigrationOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "mgn:StartNetworkMigrationAnalysis",
        "mgn:StartNetworkMigrationCodeGeneration",
        "mgn:StartNetworkMigrationDeployedStacksDeletion",
        "mgn:StartNetworkMigrationDeployment",
        "mgn:StartNetworkMigrationMapping"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "OrganizationsOperationsReadOnlyNetworkMigration",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RamShareCrossAccountOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "RamViaCfnShareAssociateOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService",
          "ram:RequestedResourceType" : [
            "ec2:TransitGateway",
            "ssm:Parameter"
          ]
        }
      }
    },
    {
      "Sid" : "RamViaCfnShareCreate",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ram:CreateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "Bool" : {
          "ram:RequestedAllowsExternalPrincipals" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RamViaCfnShareOperations",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare",
        "ram:DisassociateResourceShare",
        "ram:UpdateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "RamViaCfnShareTagOperationsWrite",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ram:TagResource"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "ReachabilityAnalyzerAnalysisStart",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:StartNetworkInsightsAnalysis"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-insights-analysis/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReachabilityAnalyzerCleanupOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteNetworkInsightsAnalysis",
        "ec2:DeleteNetworkInsightsPath",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "ReachabilityAnalyzerCreateWithRequestTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsPath",
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "ReachabilityAnalyzerCreateWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsPath",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:StartNetworkInsightsAnalysis"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "ReachabilityAnalyzerCrossOrgPathCreate",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateNetworkInsightsPath"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        }
      }
    },
    {
      "Sid" : "ReachabilityAnalyzerOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpcEndpointServiceConfigurations",
```

```
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
```

```
      "Sid" : "ReachabilityAnalyzerProbeCreateOnSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReachabilityAnalyzerSecurityGroupCreateOnVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "ReachabilityAnalyzerSecurityGroupCreateWithRequestTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group-rule/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "S3TargetBucketOperationsNetworkMigration",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:ListBucket",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::transform-vmware-target-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3TargetObjectOperationsNetworkMigration",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectAttributes",
        "s3:GetObjectVersion",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::transform-vmware-target-*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SsmParametersViaCfnOperationsReadOnly",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/network-migration/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "SsmParametersViaCfnOperationsWriteWithRequestTag",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/network-migration/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "SsmParametersViaCfnOperationsWriteWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter",
        "ssm:DeleteResourcePolicy",
        "ssm:ListTagsForResource"
```

```
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/network-migration/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "SsmParametersViaCfnRamSharingOperations",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetResourcePolicies",
        "ssm:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/network-migration/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "StsCrossAccountAssumeRoleNetworkMigration",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AWSTransformNetworkMigrationAgentSharingRole_
${aws:PrincipalAccount}",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}",
          "sts:ExternalId" : "${aws:PrincipalAccount}:workspace/${aws:PrincipalTag/
WorkspaceId}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSTransformRevenueAttributionPolicy

Deskripsi: Mengaktifkan layanan AWS Transform untuk mengelola atribusi pendapatan pelanggan untuk insentif.

`AWSTransformRevenueAttributionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTransformRevenueAttributionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Juli 2026, 16:42 UTC
- Waktu teredit: 07 Juli 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformRevenueAttributionPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PartnerCentralRevenueManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetRevenueAttribution",
        "partnercentral:UpdateRevenueAttribution",
        "partnercentral:CreateRevenueAttribution",
        "partnercentral:ListRevenueAttributions"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/revenue-attribution/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSTransformSecretsManagerConnectorPolicy

Deskripsi: Mengaktifkan layanan AWS Transform untuk membaca SecretsManager Rahasia tertentu sehubungan dengan kunci KMS tertentu. Kebijakan ini memberikan izin untuk membaca nilai rahasia yang ditentukan dan mendekripsinya jika rahasia dienkripsi

`AWSTransformSecretsManagerConnectorPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTransformSecretsManagerConnectorPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Maret 2026, 21:12 UTC
- Waktu teredit: 04 Maret 2026, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformSecretsManagerConnectorPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadSecretsManagerSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
```

```
      "Resource" : "arn:aws:secretsmanager:*:*:secret:${aws:PrincipalTag/SecretId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DecryptWithCustomerProvidedKMSKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KMSKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:
${aws:RequestedRegion}:${aws:PrincipalAccount}:secret:${aws:PrincipalTag/SecretId}",
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DescribeKMSKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSTransformSecurityAgentExecutorAccess

Deskripsi: Memberikan AWS Transform (ATX) Continuous Modernis CLI/agent ation izin yang diperlukan untuk memanggil layanan Agen AWS Keamanan untuk tinjauan dan remediasi keamanan kode otomatis, termasuk mengunggah artefak pemindaian dan mengambil temuan.

`AWSTransformSecurityAgentExecutorAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTransformSecurityAgentExecutorAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Juni 2026, 21:27 UTC
- Waktu teredit: 28 Juli 2026, 15:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformSecurityAgentExecutorAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityAgentApi",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:ListAgentSpaces",
        "securityagent:CreateCodeReview",
        "securityagent:StartCodeReviewJob",
        "securityagent:ListCodeReviewJobsForCodeReview",
        "securityagent:ListFindings",
        "securityagent:BatchGetFindings",
        "securityagent:StartCodeRemediation"
      ],
      "Resource" : "arn:aws:securityagent:*:*:agent-space*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3SecurityAgentBucketRead",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::atx-security-agent-*",
        "arn:aws:s3:::atx-security-agent-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3SecurityAgentUpload",
```

```
      "Effect" : "Allow",
      "Action" : "s3:PutObject",
      "Resource" : "arn:aws:s3:::atx-security-agent-*/security-scans/*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassSecurityAgentRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/security-agent-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "securityagent.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CFNDiscoverSecurityAgentStack",
      "Effect" : "Allow",
      "Action" : "cloudformation:ListStacks",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CFNDescribeSecurityAgentStack",
      "Effect" : "Allow",
      "Action" : "cloudformation:DescribeStacks",
      "Resource" : "arn:aws:cloudformation:*:*:stack/AtxSecurityAgentStack-*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSTransformServerMigrationAgentPolicy

Deskripsi: Memberikan izin untuk AWS Transform untuk melakukan operasi migrasi server termasuk replikasi, pengujian, dan cutover menggunakan Layanan Migrasi AWS Aplikasi

`AWSTransformServerMigrationAgentPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTransformServerMigrationAgentPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Agustus 2026, 15:27 UTC
- Waktu teredit: 01 September 2026, 10:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformServerMigrationAgentPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2LaunchTemplateOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "Ec2OperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "Ec2TagOnCreateServerMigration",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnInstanceLifecycleOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CreateSnapshot",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteVolume",
        "ec2:DetachVolume",
        "ec2:ModifyInstanceAttribute",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnInstanceProvisionCreateWithRequestTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateVolume",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnLaunchOnSharedVpc",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedFor" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnLaunchOnWorkspaceVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedFor" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:GetSubnetCidrReservations",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnRunInstancesOnAmsSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*"
```

```
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnRunInstancesOnImage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnRunInstancesOnSg",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
```

```
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnSecurityGroupCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnTagOnCreateSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
```

```
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateSnapshot",
            "CreateVolume",
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnVolumeFromSnapshotCreate",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "ec2:Owner" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "FsxOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "FsxViaMgnDescribeOperations",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeVolumes",
        "fsx:DescribeSnapshots"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "FsxViaMgnCreateVolume",
      "Effect" : "Allow",
      "Action" : "fsx:CreateVolume",
      "Resource" : [
        "arn:aws:fsx:*:*:volume/*/*",
        "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "FsxViaMgnDeleteVolumeAndTag",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteVolume",
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
```

```
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "FsxViaMgnCreateSnapshot",
      "Effect" : "Allow",
      "Action" : "fsx:CreateSnapshot",
      "Resource" : [
        "arn:aws:fsx:*:*:snapshot/*/*",
        "arn:aws:fsx:*:*:volume/*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IamViaMgnEc2PassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithDrsRole",
```

```
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KmsS3EncryptionOperationsServerMigration",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/EncryptionKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "MgnAccountSettingsOperations",
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetAccountSettings",
        "mgn:RegisterAgentForMgn",
        "mgn:UpdateAccountSettings"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
```

```
    },
    {
      "Sid" : "MgnAppWaveCreate",
      "Effect" : "Allow",
      "Action" : [
        "mgn:CreateApplication",
        "mgn:CreateWave"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "MgnAppWaveServerTagOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "mgn:TagResource"
      ],
      "Resource" : [
        "arn:aws:mgn:*:*:application/*",
        "arn:aws:mgn:*:*:source-server/*",
        "arn:aws:mgn:*:*:wave/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "MgnImportExportOperationWrite",
      "Effect" : "Allow",
      "Action" : [
        "mgn:StartExport",
        "mgn:StartImport",
```

```
        "mgn:StartImportFileEnrichment"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "MgnImportExportTagOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "mgn:TagResource"
      ],
      "Resource" : [
        "arn:aws:mgn:*:*:export/*",
        "arn:aws:mgn:*:*:import/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "mgn:CreateAction" : [
            "StartExport",
            "StartImport"
          ]
        }
      }
    },
    {
      "Sid" : "MgnJobAndErrorOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "mgn:DescribeJobLogItems",
        "mgn:ListExportErrors",
        "mgn:ListImportErrors"
      ],
      "Resource" : [
        "arn:aws:mgn:*:*:export/*",
        "arn:aws:mgn:*:*:import/*",
        "arn:aws:mgn:*:*:job/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "MgnJobTagOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "mgn:TagResource"
      ],
      "Resource" : "arn:aws:mgn:*:*:job/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "mgn:CreateAction" : [
            "StartCutover",
            "StartTest",
            "TerminateTargetInstances"
          ]
        }
      }
    },
    {
      "Sid" : "MgnSourceServerLifecycleOperations",
      "Effect" : "Allow",
      "Action" : [
        "mgn:ChangeServerLifecycleState",
        "mgn:FinalizeCutover",
        "mgn:GetReplicationConfiguration",
        "mgn:ListSourceServerActions",
        "mgn:ListTagsForResource",
        "mgn:MarkAsArchived",
        "mgn:PauseReplication",
        "mgn:PutSourceServerAction",
        "mgn:RemoveSourceServerAction",
```

```
        "mgn:ResumeReplication",
        "mgn:StartCutover",
        "mgn:StartReplication",
        "mgn:StartTest",
        "mgn:StopReplication",
        "mgn:UpdateReplicationConfiguration",
        "mgn:UpdateSourceServer"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "OrganizationsOperationsReadOnlyServerMigration",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PostLaunchAutomationMonitoring",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "S3AgentSignatureOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::aws-application-migration-service-*/latest/source-
automation-client/linux/ssaf-client/ssaf_client.sig"
    },
    {
      "Sid" : "S3TargetBucketOperationsServerMigration",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:ListBucket",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::transform-vmware-target-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3TargetObjectOperationsServerMigration",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectAttributes",
        "s3:GetObjectVersion",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::transform-vmware-target-*/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "ServerMigrationOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "mgn:DescribeJobs",
        "mgn:DescribeLaunchConfigurationTemplates",
        "mgn:DescribeReplicationConfigurationTemplates",
        "mgn:DescribeReplicationServerAssociationsForMgn",
        "mgn:DescribeSourceServers",
        "mgn:DescribeVcenterClients",
        "mgn:GetLaunchConfiguration",
        "mgn:ListApplications",
        "mgn:ListConnectors",
        "mgn:ListExports",
        "mgn:ListImportFileEnrichments",
        "mgn:ListImports",
        "mgn:ListTemplateActions",
        "mgn:ListWaves"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
```

```
    {
      "Sid" : "ServerMigrationOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "mgn:AssociateApplications",
        "mgn:AssociateSourceServers",
        "mgn:DeleteApplication",
        "mgn:DeleteWave",
        "mgn:DisassociateApplications",
        "mgn:DisassociateSourceServers",
        "mgn:TerminateTargetInstances",
        "mgn:UpdateApplication",
        "mgn:UpdateLaunchConfiguration",
        "mgn:UpdateWave"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "ServerMigrationTemplateOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "mgn:PutTemplateAction",
        "mgn:RemoveTemplateAction",
        "mgn:UpdateLaunchConfigurationTemplate",
        "mgn:UpdateReplicationConfigurationTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ServiceQuotasViaMgnOperationsReadOnly",
      "Effect" : "Allow",
```

```
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "arn:aws:servicequotas:*:*:vpc/L-2AFB9258",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SsmAgentCommandOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "SsmAgentCommandOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
```

```
          "aws:ResourceTag/CreatedFor" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "SsmDocumentListOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "SsmDocumentOnAwsManagedOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument",
        "ssm:ListDocumentVersions"
      ],
      "Resource" : "arn:aws:ssm:*::document/AWS*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "SsmDocumentOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument",
        "ssm:ListDocumentVersions"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SsmMigrationDocumentOperations",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:SendCommand"
      ],
      "Resource" : "arn:aws:ssm:*::document/AWSMigration-RunSourceServerAction",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "SsmParameterServerMigrationOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameters",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SsmViaMgnPostLaunchCommandAndAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
```

```
        "arn:aws:ssm:*:*:automation-definition/*:*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:document/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SsmViaMgnPostLaunchCommandAndAutomationOnAwsManaged",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*::automation-definition/AWS*:*",
        "arn:aws:ssm:*::document/AWS*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "SsmViaMgnPostLaunchSendCommandToInstances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "StsCrossAccountAssumeRole",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AWSTransformRehostSharingRole_
${aws:PrincipalAccount}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}",
          "sts:ExternalId" : "${aws:PrincipalAccount}:workspace/${aws:PrincipalTag/
WorkspaceId}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSTrustedAdvisorPriorityFullAccess

Deskripsi: Menyediakan akses penuh ke Priorit AWS as Penasihat Tepercaya. Kebijakan ini juga memungkinkan pengguna untuk menambahkan Penasihat Tepercaya sebagai layanan tepercaya dengan AWS Organisasi dan untuk menentukan akun administrator yang didelegasikan untuk Prioritas Penasihat Tepercaya.

`AWSTrustedAdvisorPriorityFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTrustedAdvisorPriorityFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 Agustus 2022, 16:08 UTC
- Waktu teredit: 16 Agustus 2022, 16:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "trustedadvisor:DescribeAccount*",
        "trustedadvisor:DescribeOrganization",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:DownloadRisk",
        "trustedadvisor:UpdateRiskStatus",
        "trustedadvisor:DescribeNotificationConfigurations",
        "trustedadvisor:UpdateNotificationConfigurations",
        "trustedadvisor:DeleteNotificationConfigurationForDelegatedAdmin",
        "trustedadvisor:SetOrganizationAccess"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "reporting.trustedadvisor.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
      "Condition" : {
        "StringLike" : {
```

```
          "iam:AWSServiceName" : "reporting.trustedadvisor.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "reporting.trustedadvisor.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSTrustedAdvisorPriorityReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke Prioritas Penasihat AWS Tepercaya. Ini termasuk izin untuk melihat akun administrator yang didelegasikan.

`AWSTrustedAdvisorPriorityReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSTrustedAdvisorPriorityReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 Agustus 2022, 16:35 UTC
- Waktu teredit: 16 Agustus 2022, 16:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeAccount*",
        "trustedadvisor:DescribeOrganization",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:DownloadRisk",
        "trustedadvisor:DescribeNotificationConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "reporting.trustedadvisor.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSTrustedAdvisorReportingServiceRolePolicy

Deskripsi: Kebijakan Layanan untuk Pel Multi-account aporan Penasihat Tepercaya

`AWSTrustedAdvisorReportingServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 19 November 2019, 17:41 UTC

- Waktu teredit: 28 Februari 2023, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSTrustedAdvisorServiceRolePolicy

Deskripsi: Akses Layanan AWS Penasihat Tepercaya untuk membantu mengurangi biaya, meningkatkan kinerja, dan meningkatkan keamanan AWS lingkungan Anda.

`AWSTrustedAdvisorServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 22 Februari 2018, 21:24 UTC
- Waktu yang diedit: 14 Mei 2026, 21:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedAdvisorServiceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ListAnalyzers",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
```

```
        "autoscaling:DescribeLaunchConfigurations",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudfront:ListDistributions",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetTrail",
        "cloudtrail:ListTrails",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "dax:DescribeClusters",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeImages",
        "ec2:DescribeNatGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:GetManagedPrefixListEntries",
        "ecs:DescribeTaskDefinition",
        "ecs:ListTaskDefinitions",
        "ecs:ListClusters",
        "ecs:ListTasks",
        "ecs:DescribeTasks",
        "ecs:ListTaskDefinitionFamilies",
        "elasticloadbalancing:DescribeAccountLimits",
```

```
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "iam:GenerateCredentialReport",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetServerCertificate",
        "iam:ListServerCertificates",
        "iam:ListSAMLProviders",
        "kinesis:DescribeLimits",
        "kafka:DescribeClusterV2",
        "kafka:ListClustersV2",
        "kafka:ListNodes",
        "network-firewall:ListFirewalls",
        "network-firewall:DescribeFirewall",
        "outposts:ListAssets",
        "outposts:GetOutpost",
        "outposts:ListOutposts",
        "rds:DescribeAccountAttributes",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroupOptions",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribeReservedDBInstances",
        "rds:DescribeReservedDBInstancesOfferings",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters",
        "redshift:DescribeReservedNodeOfferings",
```

```
        "redshift:DescribeReservedNodes",
        "route53:GetAccountLimit",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverEndpointIpAddresses",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetLifecycleConfiguration",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "ses:GetSendQuota",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSUserAttributeCostAllocationPolicy

Deskripsi: Menyediakan akses baca-saja ke atribut pengguna dari Pusat Identitas AWS IAM untuk atribut pengguna yang telah dipilih pelanggan.

`AWSUserAttributeCostAllocationPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 15 Desember 2025, 16:34 UTC
- Waktu teredit: 15 Desember 2025, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserAttributeCostAllocationPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/user-attribute-cost-
allocation-data.amazonaws.com/AWSServiceRoleForUserAttributeCostAllocation"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSUserNotificationsServiceLinkedRolePolicy

Deskripsi: Mengiz AWS inkan Pemberitahuan Pengguna untuk memanggil AWS layanan atas nama Anda.

`AWSUserNotificationsServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 19 April 2023, 13:28 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
```

```
        "events:ListTargetsByRule",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AWSUserNotificationsManagedRule-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Notifications"
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrgsActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListParents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAdminDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "notifications.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "OrganizationNotificationConfigurationDistribution",
      "Effect" : "Allow",
      "Action" : [
        "notifications:CreateNotificationConfiguration",
        "notifications:DeleteNotificationConfiguration",
        "notifications:CreateEventRule",
        "notifications:UpdateEventRule",
        "notifications:DeleteEventRule"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSVendorInsightsAssessorFullAccess

Deskripsi: Menyediakan akses penuh untuk melihat sumber daya Vendor Wawasan yang berjudul dan mengelola langganan Vendor Insights

`AWSVendorInsightsAssessorFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSVendorInsightsAssessorFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juli 2022, 15:05 UTC
- Waktu teredit: 01 Desember 2022, 00:51 UTC

- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetProfileAccessTerms",
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreateAgreementRequest",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:AcceptAgreementRequest",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:CancelAgreement"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:AgreementType" : "VendorInsightsAgreement"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSVendorInsightsAssessorReadOnly

Deskripsi: Menyediakan akses baca-saja untuk melihat sumber daya Vendor Insights yang berjudul

`AWSVendorInsightsAssessorReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSVendorInsightsAssessorReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juli 2022, 15:05 UTC
- Waktu teredit: 01 Desember 2022, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSVendorInsightsVendorFullAccess

Deskripsi: Menyediakan akses penuh untuk membuat dan mengelola sumber daya Vendor Insights

`AWSVendorInsightsVendorFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSVendorInsightsVendorFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juli 2022, 15:05 UTC
- Waktu teredit: 19 Oktober 2023, 01:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:DescribeEntity",
      "Resource" : "arn:aws:aws-marketplace:*:*:*/SaaSProduct/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:ListEntities",
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:CreateDataSource",
        "vendor-insights:UpdateDataSource",
        "vendor-insights:DeleteDataSource",
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:CreateSecurityProfile",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:AssociateDataSource",
        "vendor-insights:DisassociateDataSource",
        "vendor-insights:UpdateSecurityProfile",
        "vendor-insights:ActivateSecurityProfile",
        "vendor-insights:DeactivateSecurityProfile",
        "vendor-insights:UpdateSecurityProfileSnapshotCreationConfiguration",
        "vendor-insights:UpdateSecurityProfileSnapshotReleaseConfiguration",
        "vendor-insights:ListSecurityProfileSnapshots",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:TagResource",
        "vendor-insights:UntagResource",
        "vendor-insights:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:CancelAgreement",
        "aws-marketplace:SearchAgreements"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:AgreementType" : "VendorInsightsAgreement"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSVendorInsightsVendorReadOnly

Deskripsi: Menyediakan akses baca-saja untuk melihat sumber daya Vendor Insights

`AWSVendorInsightsVendorReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSVendorInsightsVendorReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juli 2022, 15:05 UTC
- Waktu teredit: 01 Desember 2022, 00:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:DescribeEntity",
      "Resource" : "arn:aws:aws-marketplace:*:*:*/SaaSProduct/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:ListEntities",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots",
        "vendor-insights:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
```

```
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSVPCFlowLogsServiceRolePolicy

Deskripsi: Memberikan izin untuk mengontrol sumber daya yang dikelola layanan dan memanggil API yang diperlukan untuk pengayaan bidang log atas nama pelanggan.

`AWSVPCFlowLogsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 11 Mei 2026, 15:57 UTC
- Waktu teredit: 11 Mei 2026, 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCFlowLogsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutRuleOnSpecificSourcesAndDetailTypes",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : [
        "arn:aws:events:*:*:rule/VPCFlowLogsEC2TagsManagedRule",
        "arn:aws:events:*:*:rule/VPCFlowLogsASGTagsManagedRule"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.tag",
            "aws.autoscaling"
          ],
          "events:detail-type" : [
            "AWS API Call via CloudTrail",
            "Tag Change on Resource"
          ]
        },
        "Null" : {
          "events:source" : "false",
          "events:detail-type" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowOtherOperationsOnRulesManagedByVPCFlowLogs",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
```

```
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/VPCFlowLogsEC2TagsManagedRule",
        "arn:aws:events:*:*:rule/VPCFlowLogsASGTagsManagedRule"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDescribeTagsOnAllEC2Resources",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "autoscaling:DescribeTags"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSVpcLatticeServiceRolePolicy

Deskripsi: Mengizinkan VPC Lattice mengakses AWS sumber daya atas nama Anda.

`AWSVpcLatticeServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 30 November 2022, 20:47 UTC
- Waktu teredit: 01 Desember 2024, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/VpcLattice"
        }
      }
    },
    {
      "Sid" : "VpcLatticeDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "VpcLatticeCreateNetworkInterfaceWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/VpcLatticeManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VpcLatticeCreateNetworkInterfaceWithSubnetAndSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "VpcLatticeTagNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "VpcLatticeMutateNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
```

```
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VpcLatticeManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VpcLatticeModifyNetworkInterfaceSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "VpcLatticeModifyNetworkInterfaceActionsIpAddressActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VpcLatticeManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VpcLatticeAssociateHostedZoneToVpc",
      "Effect" : "Allow",
      "Action" : [
        "route53:AssociateVPCWithHostedZone"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSVPCS2SVpnServiceRolePolicy

Deskripsi: Izinkan Site-to-Site VPN membuat dan mengelola sumber daya yang terkait dengan Koneksi VPN Anda.

`AWSVPCS2SVpnServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 06 Agustus 2019, 14:13 UTC
- Waktu teredit: 15 Mei 2025, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "0",
      "Effect" : "Allow",
      "Action" : [
        "acm:ExportCertificate",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpnConnectionSecretsManagement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:s2svpn!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "s2svpn",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "VpnConnectionSecretsCreation",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:s2svpn!*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "s2svpn!*"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSVPCTransitGatewayServiceRolePolicy

Deskripsi: Izinkan VPC Transit Gateway membuat dan mengelola sumber daya yang diperlukan untuk Lampiran VPC Transit Gateway Anda.

`AWSVPCTransitGatewayServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 26 November 2018, 16:21 UTC
- Waktu teredit: 15 April 2021, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:AssignIpv6Addresses",
        "ec2:UnAssignIpv6Addresses"
      ],
      "Resource" : "*",
      "Effect" : "Allow",
      "Sid" : "0"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSVPCVerifiedAccessServiceRolePolicy

Deskripsi: Kebijakan untuk mengaktifkan layanan Akses Ter AWS verifikasi untuk menyediakan titik akhir atas nama Anda

`AWSVPCVerifiedAccessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 29 November 2022, 03:35 UTC

- Waktu teredit: 17 November 2023, 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VerifiedAccessRoleModifyTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VerifiedAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VerifiedAccessRoleModifyNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "VerifiedAccessRoleNetworkInterfaceActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "VerifiedAccessRoleTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/VerifiedAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VerifiedAccessRoleTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSWAFConsoleFullAccess

Deskripsi: Menyediakan akses penuh ke AWS WAF melalui. Konsol Manajemen AWS Perhatikan bahwa kebijakan ini juga memberikan izin untuk membuat daftar dan memperbarui CloudFront distribusi Amazon, izin untuk melihat penyeimbang beban di AWS Elastic Load Balancing, izin untuk melihat API dan tahapan REST Amazon API Gateway, izin untuk membuat daftar dan melihat CloudWatch metrik Amazon, dan izin untuk melihat wilayah yang diaktifkan dalam akun.

`AWSWAFConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSWAFConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 April 2020, 18:38 UTC
- Waktu teredit: 01 Juli 2026, 04:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v22 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowUseOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:*",
```

```
        "waf-regional:*"
      ],
      "Resource" : [
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf:*:*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
      "Sid" : "AllowUseOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:*"
```

```
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
      "Sid" : "AllowDisassociateWebACL",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3ListAllMyBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2DescribeRegions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowActionsForCloudFront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetDistribution",
        "cloudfront:UpdateDistribution",
        "cloudfront:AssociateDistributionWebACL",
        "cloudfront:DisassociateDistributionWebACL"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid" : "AllowListActionsForCloudFront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionTenant",
        "cloudfront:AssociateDistributionTenantWebACL",
        "cloudfront:DisassociateDistributionTenantWebACL"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution-tenant/*"
    },
    {
      "Sid" : "AllowListActionsForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListDistributionTenantsByCustomization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:SetWebAcl",
```

```
        "elasticloadbalancing:CreateWebACLAssociation",
        "elasticloadbalancing:DeleteWebACLAssociation",
        "elasticloadbalancing:GetLoadBalancerWebACL"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "AllowListActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeWebACLAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:SetWebACL"
      ],
      "Resource" : "arn:aws:apigateway:*::/restapis/*/stages/*"
    },
    {
      "Sid" : "AllowListActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "arn:aws:apigateway:*::/*"
    },
    {
      "Sid" : "AllowActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:SetWebACL",
        "appsync:AssociateWebACL",
        "appsync:DisassociateWebACL",
        "appsync:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:appsync:*:*:apis/*"
    },
    {
      "Sid" : "AllowListActionsForAppSync",
```

```
      "Effect" : "Allow",
      "Action" : [
        "appsync:ListGraphqlApis",
        "appsync:ListApis",
        "appsync:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:AssociateWebACL",
        "cognito-idp:DisassociateWebACL",
        "cognito-idp:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListUserPools",
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:AssociateWebAcl",
        "apprunner:DisassociateWebAcl",
        "apprunner:DescribeWebAclForService"
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateVerifiedAccessInstanceWebAcl",
        "ec2:DisassociateVerifiedAccessInstanceWebAcl",
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
    {
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:AssociateWebACL",
        "amplify:DisassociateWebACL",
        "amplify:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogQueryActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:StartQuery",
        "logs:DescribeQueryDefinitions",
        "logs:GetQueryResults"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:aws-waf-logs-*"
    },
    {
      "Sid" : "AllowLogGroupDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogDeliverySubscription",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForS3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForCloudWatchLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowListActionForFirehoseStream",
      "Effect" : "Allow",
      "Action" : [
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForPricing",
      "Effect" : "Allow",
      "Action" : [
        "pricing:ListPriceLists",
        "pricing:GetPriceListFileUrl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowMarketplaceViewSubscriptions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:GetSubscription",
        "pricingplanmanager:UpdateSubscription",
        "pricingplanmanager:CancelSubscription",
        "pricingplanmanager:CancelSubscriptionChange"
      ],
      "Resource" : "arn:aws:pricingplanmanager::*:subscription:*"
    },
    {
      "Sid" : "AllowListActionsForRoute53",
```

```
      "Effect" : "Allow",
      "Action" : [
        "route53:ListHostedZones",
        "route53:GetHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : "pricingplanmanager:ListSubscriptions",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayAssociateWebACL",
        "bedrock-agentcore:GatewayDisassociateWebACL",
        "bedrock-agentcore:GatewayGetWebACLForResource",
        "bedrock-agentcore:GetGateway"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:gateway/*"
    },
    {
      "Sid" : "AllowListActionsForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayListResourcesForWebACL",
        "bedrock-agentcore:ListGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSWAFConsoleReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke AWS WAF melalui. Konsol Manajemen AWS Perhatikan bahwa kebijakan ini juga memberikan izin untuk membuat daftar CloudFront distribusi Amazon, izin untuk melihat penyeimbang beban di AWS Elastic Load Balancing, izin untuk melihat API dan tahapan REST Amazon API Gateway, izin untuk membuat daftar dan melihat CloudWatch metrik Amazon, dan izin untuk melihat wilayah yang diaktifkan dalam akun.

`AWSWAFConsoleReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSWAFConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 April 2020, 18:43 UTC
- Waktu teredit: 01 Juli 2026, 04:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v21 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:Get*",
```

```
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*"
      ],
      "Resource" : [
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf:*:*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
      "Sid" : "AllowReadOnlyOfAWSWAF",
      "Effect" : "Allow",
```

```
      "Action" : [
        "wafv2:Get*",
        "wafv2:List*",
        "wafv2:Describe*",
        "wafv2:CheckCapacity"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
      "Sid" : "AllowEC2DescribeRegions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForCloudFront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid" : "AllowListActionsForCloudFront",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionTenant"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution-tenant/*"
    },
    {
      "Sid" : "AllowListActionsForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListDistributionTenantsByCustomization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:GetLoadBalancerWebACL"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "AllowListActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeWebACLAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
```

```
        "apigateway:GET"
      ],
      "Resource" : "arn:aws:apigateway:*::/*"
    },
    {
      "Sid" : "AllowGetActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:appsync:*:*:apis/*"
    },
    {
      "Sid" : "AllowListActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:ListGraphqlApis",
        "appsync:ListApis",
        "appsync:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListUserPools",
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:DescribeWebAclForService"
```

```
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
    {
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "amplify:ListResourcesForWebACL"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3ListAllMyBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogGroupDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionForFirehoseStream",
      "Effect" : "Allow",
      "Action" : [
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForPricing",
      "Effect" : "Allow",
      "Action" : [
        "pricing:ListPriceLists",
        "pricing:GetPriceListFileUrl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowMarketplaceViewSubscriptions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowLogQueryActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:DescribeQueryDefinitions",
        "logs:GetQueryResults"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:aws-waf-logs-*"
    },
    {
      "Sid" : "AllowListActionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:GetSubscription"
      ],
      "Resource" : "arn:aws:pricingplanmanager::*:subscription:*"
    },
    {
      "Sid" : "AllowListActionsForRoute53",
      "Effect" : "Allow",
      "Action" : [
        "route53:ListHostedZones",
        "route53:GetHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListSubscriptionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:ListSubscriptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayGetWebACLForResource",
        "bedrock-agentcore:GetGateway"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:gateway/*"
    },
```

```
    {
      "Sid" : "AllowListActionsForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayListResourcesForWebACL",
        "bedrock-agentcore:ListGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSWAFFullAccess

Deskripsi: Menyediakan akses penuh ke tindakan AWS WAF.

`AWSWAFFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSWAFFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Oktober 2015, 20:44 UTC
- Waktu teredit: 28 Juli 2026, 21:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFFullAccess`

Versi kebijakan

Versi kebijakan: v17 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowUseOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:*",
        "waf-regional:*"
      ],
      "Resource" : [
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf::*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
```

```
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
      "Sid" : "AllowUseOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:*"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
      "Sid" : "AllowDisassociateWebACL",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeWebACLAssociation"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:SetWebAcl",
        "elasticloadbalancing:CreateWebACLAssociation",
        "elasticloadbalancing:DeleteWebACLAssociation",
        "elasticloadbalancing:GetLoadBalancerWebACL"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "AllowActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:SetWebACL"
      ],
      "Resource" : "arn:aws:apigateway:*::/restapis/*/stages/*"
    },
    {
      "Sid" : "AllowListActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:SetWebACL",
        "appsync:AssociateWebACL",
        "appsync:DisassociateWebACL",
        "appsync:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:appsync:*:*:apis/*"
    },
    {
      "Sid" : "AllowActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:AssociateWebACL",
        "cognito-idp:DisassociateWebACL",
```

```
        "cognito-idp:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:AssociateWebAcl",
        "apprunner:DisassociateWebAcl",
        "apprunner:DescribeWebAclForService"
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateVerifiedAccessInstanceWebAcl",
        "ec2:DisassociateVerifiedAccessInstanceWebAcl",
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
    {
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:AssociateWebACL",
        "amplify:DisassociateWebACL",
        "amplify:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogGroupDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogDeliverySubscription",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForS3Bucket",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForCloudWatchLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowActionsForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayAssociateWebACL",
        "bedrock-agentcore:GatewayDisassociateWebACL",
        "bedrock-agentcore:GatewayGetWebACLForResource"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:gateway/*"
    },
    {
      "Sid" : "AllowListActionsForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayListResourcesForWebACL"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSWAFReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke tindakan AWS WAF.

`AWSWAFReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSWAFReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Oktober 2015, 20:43 UTC
- Waktu teredit: 01 Juli 2026, 04:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v13 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "AllowReadOnlyOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*"
      ],
      "Resource" : [
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf::*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
```

```
    },
    {
      "Sid" : "AllowReadOnlyOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:Get*",
        "wafv2:List*",
        "wafv2:Describe*",
        "wafv2:CheckCapacity"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
      "Sid" : "AllowGetActionForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:DescribeWebAclForService"
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
```

```
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
    {
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetWebACLForResource"
```

```
      ],
      "Resource" : "arn:aws:appsync:*:*:apis/*"
    },
    {
      "Sid" : "AllowListActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionsForELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:GetLoadBalancerWebACL"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "AllowListActionsForELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeWebACLAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadActionsForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayGetWebACLForResource"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:gateway/*"
    },
    {
      "Sid" : "AllowListActionsForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayListResourcesForWebACL"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSWellArchitectedAgentOrganizationsServiceRolePolicy

Deskripsi: Men AWS Well-Architected gizinkan Agen mengakses struktur organisasi dan informasi administrator yang didelegasikan di AWS Organisasi atas nama Anda

`AWSWellArchitectedAgentOrganizationsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 15 September 2026, 18:37 UTC
- Waktu teredit: 15 September 2026, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedAgentOrganizationsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSWellArchitectedAgentResourceScanningServiceRolePolicy

Deskripsi: Memberikan akses read-only kepada AWS Well-Architected Agen ke konfigurasi AWS sumber daya, pengaturan keamanan, dan data operasional untuk menghasilkan rekomendasi pengoptimalan

`AWSWellArchitectedAgentResourceScanningServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 04 Agustus 2026, 17:27 UTC
- Waktu teredit: 24 September 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedAgentResourceScanningServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WellArchitectedAgentScanningReadOnly1",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "aco-automation:GetAutomationRule",
        "aco-automation:ListAutomationRules",
```

```
        "aidevops:DescribePrivateConnection",
        "aidevops:GetAgentSpace",
        "aidevops:GetAssociation",
        "aidevops:GetOperatorApp",
        "aidevops:GetService",
        "aidevops:ListAgentSpaces",
        "aidevops:ListAssociations",
        "aidevops:ListPrivateConnections",
        "aidevops:ListServices",
        "aidevops:ListTagsForResource",
        "aiops:GetInvestigationGroup",
        "aiops:GetInvestigationGroupPolicy",
        "aiops:ListInvestigationGroups",
        "aiops:ListTagsForResource",
        "airflow-serverless:GetWorkflow",
        "airflow-serverless:ListTagsForResource",
        "airflow-serverless:ListWorkflows",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListTagsForResource",
        "amplifyuibuilder:GetComponent",
        "amplifyuibuilder:GetForm",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListComponents",
        "amplifyuibuilder:ListForms",
        "amplifyuibuilder:ListThemes",
        "aoss:BatchGetCollection",
        "aoss:BatchGetCollectionGroup",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollectionGroups",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
```

```
        "aoss:ListSecurityPolicies",
        "aoss:ListTagsForResource",
        "aoss:ListVpcEndpoints",
        "apigateway:GetRoutingRule",
        "apigateway:ListRoutingRules",
        "app-integrations:GetApplication",
        "app-integrations:GetDataIntegration",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListApplications",
        "app-integrations:ListDataIntegrations",
        "app-integrations:ListEventIntegrations",
        "app-integrations:ListTagsForResource",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExtension",
        "appconfig:GetExtensionAssociation",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListDeployments",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListExtensions",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:DescribeConnector",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlow",
        "appflow:ListConnectors",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListGroupingAttributeDefinitions",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServices",
```

```
        "application-signals:ListTagsForResource",
        "applicationinsights:DescribeApplication",
        "applicationinsights:DescribeComponent",
        "applicationinsights:DescribeLogPattern",
        "applicationinsights:ListApplications",
        "applicationinsights:ListComponents",
        "applicationinsights:ListLogPatternSets",
        "applicationinsights:ListLogPatterns",
        "applicationinsights:ListTagsForResource",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListServices",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appstream:DescribeAppBlockBuilders",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeImageBuilders",
        "appstream:DescribeStacks",
        "appstream:DescribeUserStackAssociations",
        "appstream:DescribeUsers",
        "appstream:ListTagsForResource",
        "appsync:GetApi",
        "appsync:GetChannelNamespace",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
        "appsync:GetGraphqlApi",
        "appsync:GetSourceApiAssociation",
        "appsync:ListApis",
        "appsync:ListChannelNamespaces",
        "appsync:ListDataSources",
        "appsync:ListDomainNames",
        "appsync:ListFunctions",
        "appsync:ListGraphqlApis",
        "appsync:ListResolvers",
        "appsync:ListSourceApiAssociations",
        "appsync:ListTagsForResource",
        "apptest:GetTestCase",
        "apptest:ListTagsForResource",
        "apptest:ListTestCases",
```

```
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeAnomalyDetector",
        "aps:DescribeLoggingConfiguration",
        "aps:DescribeQueryLoggingConfiguration",
        "aps:DescribeResourcePolicy",
        "aps:DescribeRuleGroupsNamespace",
        "aps:DescribeScraper",
        "aps:DescribeScraperLoggingConfiguration",
        "aps:DescribeWorkspace",
        "aps:DescribeWorkspaceConfiguration",
        "aps:ListAnomalyDetectors",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListScrapers",
        "aps:ListTagsForResource",
        "aps:ListWorkspaces",
        "arc-region-switch:GetPlan",
        "arc-region-switch:ListPlans",
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListTagsForResource",
        "arc-zonal-shift:GetAutoshiftObserverNotificationStatus",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:ListManagedResources",
        "athena:GetCapacityAssignmentConfiguration",
        "athena:GetCapacityReservation",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListCapacityReservations",
        "athena:ListDataCatalogs",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "auditmanager:GetAssessment",
        "auditmanager:ListAssessments",
        "auditmanager:ListTagsForResource",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAccountSettings",
        "autoscaling:DescribeAdjustmentTypes",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeAutoScalingNotificationTypes",
        "autoscaling:DescribeInstanceRefreshes",
```

```
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHookTypes",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribeLoadBalancerTargetGroups",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeMetricCollectionTypes",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScalingProcessTypes",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeTerminationPolicyTypes",
        "autoscaling:DescribeTrafficSources",
        "autoscaling:DescribeWarmPool",
        "aws-external-anthropic:GetWorkspace",
        "aws-external-anthropic:ListTagsForResource",
        "aws-external-anthropic:ListWorkspaces",
        "b2bi:GetCapability",
        "b2bi:GetPartnership",
        "b2bi:GetProfile",
        "b2bi:GetTransformer",
        "b2bi:ListCapabilities",
        "b2bi:ListPartnerships",
        "b2bi:ListProfiles",
        "b2bi:ListTagsForResource",
        "b2bi:ListTransformers",
        "backup-gateway:GetHypervisor",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup:DescribeBackupVault",
        "backup:DescribeFramework",
        "backup:DescribeReportPlan",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:GetTieringConfiguration",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListFrameworks",
```

```
        "backup:ListReportPlans",
        "backup:ListRestoreTestingPlans",
        "backup:ListRestoreTestingSelections",
        "backup:ListTags",
        "backup:ListTieringConfigurations",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeConsumableResource",
        "batch:DescribeJobDefinitions",
        "batch:DescribeJobQueues",
        "batch:DescribeQuotaShare",
        "batch:DescribeSchedulingPolicies",
        "batch:DescribeServiceEnvironments",
        "batch:ListConsumableResources",
        "batch:ListQuotaShares",
        "batch:ListSchedulingPolicies",
        "bcm-data-exports:GetExport",
        "bcm-data-exports:ListExports",
        "bcm-data-exports:ListTagsForResource",
        "bcm-pricing-calculator:GetBillScenario",
        "bcm-pricing-calculator:ListBillScenarios",
        "bcm-pricing-calculator:ListTagsForResource",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetApiKeyCredentialProvider",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetBrowserProfile",
        "bedrock-agentcore:GetCodeInterpreter",
        "bedrock-agentcore:GetDataset",
        "bedrock-agentcore:GetEvaluator",
        "bedrock-agentcore:GetGateway",
        "bedrock-agentcore:GetGatewayTarget",
        "bedrock-agentcore:GetHarness",
        "bedrock-agentcore:GetMemory",
        "bedrock-agentcore:GetOauth2CredentialProvider",
        "bedrock-agentcore:GetOnlineEvaluationConfig",
        "bedrock-agentcore:GetPaymentConnector",
        "bedrock-agentcore:GetPaymentCredentialProvider",
        "bedrock-agentcore:GetPolicy",
        "bedrock-agentcore:GetPolicyEngine",
        "bedrock-agentcore:GetWorkloadIdentity",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListApiKeyCredentialProviders",
        "bedrock-agentcore:ListBrowserProfiles",
```

```
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListDatasets",
        "bedrock-agentcore:ListEvaluators",
        "bedrock-agentcore:ListGatewayTargets",
        "bedrock-agentcore:ListGateways",
        "bedrock-agentcore:ListHarnesses",
        "bedrock-agentcore:ListMemories",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "bedrock-agentcore:ListOnlineEvaluationConfigs",
        "bedrock-agentcore:ListPaymentConnectors",
        "bedrock-agentcore:ListPaymentCredentialProviders",
        "bedrock-agentcore:ListPolicies",
        "bedrock-agentcore:ListPolicyEngines",
        "bedrock-agentcore:ListTagsForResource",
        "bedrock-agentcore:ListWorkloadIdentities",
        "bedrock-mantle:GetProject",
        "bedrock-mantle:ListProjects",
        "bedrock-mantle:ListTagsForResource",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAutomatedReasoningPolicy",
        "bedrock:GetBlueprint",
        "bedrock:GetDataAutomationLibrary",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataSource",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetPrompt",
        "bedrock:GetPromptRouter",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListAutomatedReasoningPolicies",
        "bedrock:ListBlueprints",
```

```
        "bedrock:ListDataAutomationLibraries",
        "bedrock:ListDataAutomationProjects",
        "bedrock:ListDataSources",
        "bedrock:ListEnforcedGuardrailsConfiguration",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlowVersions",
        "bedrock:ListFlows",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListPromptRouters",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "billing:GetBillingView",
        "billing:ListBillingViews",
        "billing:ListSourceViewsForBillingView",
        "billing:ListTagsForResource",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItemVersions",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListResourcesAssociatedToCustomLineItem",
        "billingconductor:ListTagsForResource",
        "braket:ListTagsForResource",
        "braket:SearchSpendingLimits",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ListTagsForResource",
        "cases:BatchGetCaseRule",
        "cases:BatchGetField",
        "cases:GetDomain",
        "cases:GetLayout",
        "cases:GetTemplate",
        "cases:ListCaseRules",
        "cases:ListDomains",
        "cases:ListFields",
        "cases:ListLayouts",
        "cases:ListTemplates",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetAnomalyMonitors",
```

```
        "ce:GetAnomalySubscriptions",
        "ce:GetCostAndUsage",
        "ce:GetCostAndUsageWithResources",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:GetCustomAction",
        "chatbot:GetMicrosoftTeamsChannelConfiguration",
        "chatbot:ListAssociations",
        "chatbot:ListCustomActions",
        "chatbot:ListMicrosoftTeamsChannelConfigurations",
        "chatbot:ListTagsForResource",
        "chime:DescribeAppInstance",
        "chime:DescribeAppInstanceBot",
        "chime:ListAppInstanceBots",
        "chime:ListAppInstances",
        "chime:ListTagsForResource",
        "cleanrooms-ml:GetConfiguredModelAlgorithm",
        "cleanrooms-ml:GetConfiguredModelAlgorithmAssociation",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListConfiguredModelAlgorithmAssociations",
        "cleanrooms-ml:ListConfiguredModelAlgorithms",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetConfiguredTableAssociationAnalysisRule",
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListTagsForResource",
        "cloudformation:BatchDescribeTypeConfigurations",
```

```
        "cloudformation:DescribePublisher",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:ListResources",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSets",
        "cloudformation:ListStacks",
        "cloudformation:ListTypeVersions",
        "cloudformation:ListTypes",
        "cloudfront:DescribeConnectionFunction",
        "cloudfront:DescribeFunction",
        "cloudfront:DescribeKeyValueStore",
        "cloudfront:GetAnycastIpList",
        "cloudfront:GetCachePolicy",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetConnectionFunction",
        "cloudfront:GetConnectionGroup",
        "cloudfront:GetContinuousDeploymentPolicy",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetDistributionTenant",
        "cloudfront:GetFunction",
        "cloudfront:GetKeyGroup",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetOriginRequestPolicy",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:GetTrustStore",
        "cloudfront:GetVpcOrigin",
        "cloudfront:ListAnycastIpLists",
        "cloudfront:ListCachePolicies",
        "cloudfront:ListCloudFrontOriginAccessIdentities",
        "cloudfront:ListConnectionFunctions",
        "cloudfront:ListConnectionGroups",
        "cloudfront:ListContinuousDeploymentPolicies",
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListDistributions",
        "cloudfront:ListFunctions",
```

```
        "cloudfront:ListKeyGroups",
        "cloudfront:ListKeyValueStores",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListOriginRequestPolicies",
        "cloudfront:ListPublicKeys",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudfront:ListTrustStores",
        "cloudfront:ListVpcOrigins",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetChannel",
        "cloudtrail:GetDashboard",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListChannels",
        "cloudtrail:ListDashboards",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetAlarmMuteRule",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricStream",
        "cloudwatch:GetMetricWidgetImage",
        "cloudwatch:GetOTelEnrichment",
        "cloudwatch:ListAlarmMuteRules",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListManagedInsightRules",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListMetrics",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackageGroup",
        "codeartifact:DescribeRepository",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListAllowedRepositoriesForGroup",
```

```
        "codeartifact:ListDomains",
        "codeartifact:ListPackageGroups",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetFleets",
        "codebuild:ListFleets",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codeconnections:GetConnection",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codedeploy:GetApplication",
        "codedeploy:GetDeployment",
        "codedeploy:GetDeploymentConfig",
        "codedeploy:GetDeploymentGroup",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentConfigs",
        "codedeploy:ListDeploymentGroups",
        "codedeploy:ListDeployments",
        "codedeploy:ListTagsForResource",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-profiler:ListTagsForResource",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:ListTagsForResource",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "codepipeline:ListWebhooks",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:GetSyncConfiguration",
        "codestar-connections:ListConnections",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListSyncConfigurations",
        "codestar-connections:ListTagsForResource",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:ListNotificationRules",
        "cognito-identity:DescribeIdentityPool",
```

```
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeTerms",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:GetGroup",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTerms",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "comprehend:DescribeDocumentClassifier",
        "comprehend:DescribeFlywheel",
        "comprehend:DescribeResourcePolicy",
        "comprehend:ListDocumentClassifiers",
        "comprehend:ListFlywheels",
        "comprehend:ListTagsForResource",
        "config:DescribeAggregationAuthorizations",
        "config:DescribeComplianceByConfigRule",
        "config:DescribeConfigRules",
        "config:DescribeConfigurationAggregators",
        "config:DescribeConformancePacks",
        "config:DescribeOrganizationConformancePacks",
        "config:DescribeRemediationConfigurations",
        "config:GetStoredQuery",
        "config:ListStoredQueries",
        "config:ListTagsForResource",
        "connect-campaigns:DescribeCampaign",
        "connect-campaigns:ListCampaigns",
        "connect:DescribeAgentStatus",
        "connect:DescribeContactFlow",
        "connect:DescribeContactFlowModule",
        "connect:DescribeContactFlowModuleAlias",
        "connect:DescribeDataTable",
        "connect:DescribeEvaluationForm",
        "connect:DescribeHoursOfOperation",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribeNotification",
```

```
        "connect:DescribePhoneNumber",
        "connect:DescribePredefinedAttribute",
        "connect:DescribePrompt",
        "connect:DescribeQueue",
        "connect:DescribeQuickConnect",
        "connect:DescribeRoutingProfile",
        "connect:DescribeRule",
        "connect:DescribeSecurityProfile",
        "connect:DescribeTrafficDistributionGroup",
        "connect:DescribeUserHierarchyGroup",
        "connect:DescribeView",
        "connect:DescribeWorkspace",
        "connect:GetTaskTemplate",
        "connect:ListAgentStatuses",
        "connect:ListApprovedOrigins",
        "connect:ListBots",
        "connect:ListContactFlowModuleAliases",
        "connect:ListContactFlowModuleVersions",
        "connect:ListContactFlowModules",
        "connect:ListContactFlowVersions",
        "connect:ListContactFlows",
        "connect:ListDataTableAttributes",
        "connect:ListDataTables",
        "connect:ListEvaluationFormVersions",
        "connect:ListEvaluationForms",
        "connect:ListHoursOfOperationOverrides",
        "connect:ListHoursOfOperations",
        "connect:ListInstanceAttributes",
        "connect:ListInstanceStorageConfigs",
        "connect:ListInstances",
        "connect:ListIntegrationAssociations",
        "connect:ListLambdaFunctions",
        "connect:ListNotifications",
        "connect:ListPredefinedAttributes",
        "connect:ListPrompts",
        "connect:ListQueueEmailAddresses",
        "connect:ListQueueQuickConnects",
        "connect:ListQueues",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileManualAssignmentQueues",
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
        "connect:ListRules",
        "connect:ListSecurityKeys",
```

```
        "connect:ListSecurityProfileApplications",
        "connect:ListSecurityProfileFlowModules",
        "connect:ListSecurityProfilePermissions",
        "connect:ListSecurityProfiles",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListTrafficDistributionGroups",
        "connect:ListUserHierarchyGroups",
        "connect:ListUserProficiencies",
        "connect:ListUsers",
        "connect:ListViewVersions",
        "connect:ListViews",
        "connect:ListWorkspaceMedia",
        "connect:ListWorkspacePages",
        "connect:ListWorkspaces",
        "connect:SearchWorkspaceAssociations",
        "controltower:GetEnabledBaseline",
        "controltower:GetEnabledControl",
        "controltower:GetLandingZone",
        "controltower:ListEnabledBaselines",
        "controltower:ListEnabledControls",
        "controltower:ListLandingZones",
        "controltower:ListTagsForResource",
        "cur:DescribeReportDefinitions",
        "cur:ListTagsForResource",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "databrew:ListTagsForResource",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datasync:DescribeAgent",
        "datasync:DescribeLocationAzureBlob",
        "datasync:DescribeLocationEfs",
```

```
        "datasync:DescribeLocationFsxLustre",
        "datasync:DescribeLocationFsxOntap",
        "datasync:DescribeLocationFsxOpenZfs",
        "datasync:DescribeLocationFsxWindows",
        "datasync:DescribeLocationHdfs",
        "datasync:DescribeLocationNfs",
        "datasync:DescribeLocationObjectStorage",
        "datasync:DescribeLocationS3",
        "datasync:DescribeLocationSmb",
        "datasync:DescribeTask",
        "datasync:ListAgents",
        "datasync:ListLocations",
        "datasync:ListTagsForResource",
        "datasync:ListTasks",
        "datazone:GetDataSource",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentProfile",
        "datazone:GetGroupProfile",
        "datazone:GetProject",
        "datazone:GetProjectProfile",
        "datazone:GetSubscriptionTarget",
        "datazone:GetUserProfile",
        "datazone:ListConnections",
        "datazone:ListDataSources",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListDomains",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjectProfiles",
        "datazone:ListProjects",
        "datazone:ListSubscriptionTargets",
        "datazone:SearchGroupProfiles",
        "datazone:SearchUserProfiles",
        "deadline:GetFarm",
        "deadline:GetFleet",
```

```
        "deadline:GetLicenseEndpoint",
        "deadline:GetLimit",
        "deadline:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetQueueLimitAssociation",
        "deadline:GetStorageProfile",
        "deadline:ListFarms",
        "deadline:ListFleets",
        "deadline:ListLicenseEndpoints",
        "deadline:ListLimits",
        "deadline:ListMeteredProducts",
        "deadline:ListMonitors",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListQueueLimitAssociations",
        "deadline:ListQueues",
        "deadline:ListStorageProfiles",
        "deadline:ListTagsForResource",
        "detective:DescribeOrganizationConfiguration",
        "detective:GetMembers",
        "detective:ListGraphs",
        "detective:ListMembers",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "devicefarm:GetDevicePool",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:GetVPCEConfiguration",
        "devicefarm:ListDevicePools",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListNetworkProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTagsForResource",
        "devicefarm:ListTestGridProjects",
        "devicefarm:ListVPCEConfigurations",
        "devops-guru:DescribeServiceIntegration",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListNotificationChannels",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
```

```
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeLags",
        "directconnect:DescribeVirtualInterfaces",
        "dms:DescribeDataMigrations",
        "dms:DescribeReplicationConfigs",
        "dms:ListDataProviders",
        "dms:ListInstanceProfiles",
        "dms:ListMigrationProjects",
        "dms:ListTagsForResource",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:ListTagsForResource",
        "ds:DescribeDirectories",
        "ds:ListTagsForResource",
        "dsql:GetCluster",
        "dsql:GetClusterPolicy",
        "dsql:GetVpcEndpointServiceName",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeEndpoints",
        "dynamodb:DescribeExport",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeImport",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddressTransfers",
        "ec2:DescribeAddresses",
        "ec2:DescribeAddressesAttribute",
        "ec2:DescribeAggregateIdFormat",
        "ec2:DescribeAvailabilityZones",
```

```
        "ec2:DescribeAwsNetworkPerformanceMetricSubscriptions",
        "ec2:DescribeBundleTasks",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeCapacityBlockExtensionHistory",
        "ec2:DescribeCapacityBlockExtensionOfferings",
        "ec2:DescribeCapacityBlockOfferings",
        "ec2:DescribeCapacityBlockStatus",
        "ec2:DescribeCapacityBlocks",
        "ec2:DescribeCapacityManagerDataExports",
        "ec2:DescribeCapacityReservationBillingRequests",
        "ec2:DescribeCapacityReservationCancellationQuotes",
        "ec2:DescribeCapacityReservationFleets",
        "ec2:DescribeCapacityReservationTopology",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeClientVpnAuthorizationRules",
        "ec2:DescribeClientVpnConnections",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeClientVpnRoutes",
        "ec2:DescribeClientVpnTargetNetworks",
        "ec2:DescribeCoipPools",
        "ec2:DescribeConversionTasks",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDeclarativePoliciesReports",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeElasticGpus",
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeExportTasks",
        "ec2:DescribeFastLaunchImages",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DescribeFleetHistory",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeFpgaImageAttribute",
        "ec2:DescribeFpgaImages",
        "ec2:DescribeHostReservationOfferings",
        "ec2:DescribeHostReservations",
        "ec2:DescribeHosts",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeIdFormat",
        "ec2:DescribeIdentityIdFormat",
```

```
        "ec2:DescribeImageAttribute",
        "ec2:DescribeImageReferences",
        "ec2:DescribeImageUsageReportEntries",
        "ec2:DescribeImageUsageReports",
        "ec2:DescribeImages",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeImportSnapshotTasks",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceConnectEndpoints",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeInstanceEventNotificationAttributes",
        "ec2:DescribeInstanceEventWindows",
        "ec2:DescribeInstanceImageMetadata",
        "ec2:DescribeInstanceSqlHaHistoryStates",
        "ec2:DescribeInstanceSqlHaStates",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTopology",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamByoasn",
        "ec2:DescribeIpamExternalResourceVerificationTokens",
        "ec2:DescribeIpamPolicies",
        "ec2:DescribeIpamPoolAllocations",
        "ec2:DescribeIpamPools",
        "ec2:DescribeIpamPrefixListResolverTargets",
        "ec2:DescribeIpamPrefixListResolvers",
        "ec2:DescribeIpamResourceDiscoveries",
        "ec2:DescribeIpamResourceDiscoveryAssociations",
        "ec2:DescribeIpamScopes",
        "ec2:DescribeIpams",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeLockedSnapshots",
```

```
        "ec2:DescribeMacHosts",
        "ec2:DescribeMacModificationTasks",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeOutpostLags",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePrefixLists",
        "ec2:DescribePrincipalIdFormat",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeRegions",
        "ec2:DescribeReplaceRootVolumeTasks",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeReservedInstancesListings",
        "ec2:DescribeReservedInstancesModifications",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteServerEndpoints",
        "ec2:DescribeRouteServerPeers",
        "ec2:DescribeRouteServers",
        "ec2:DescribeRouteTables",
        "ec2:DescribeScheduledInstanceAvailability",
        "ec2:DescribeScheduledInstances",
        "ec2:DescribeSecondaryInterfaces",
        "ec2:DescribeSecondaryNetworks",
        "ec2:DescribeSecondarySubnets",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeServiceLinkVirtualInterfaces",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotDatafeedSubscription",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequestHistory",
```

```
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeStoreImageTasks",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilterRules",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayMeteringPolicies",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:DescribeTransitGatewayRouteTableAnnouncements",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTrunkInterfaceAssociations",
        "ec2:DescribeVerifiedAccessEndpoints",
        "ec2:DescribeVerifiedAccessGroups",
        "ec2:DescribeVerifiedAccessInstanceLoggingConfigurations",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessTrustProviders",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcBlockPublicAccessExclusions",
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEncryptionControls",
        "ec2:DescribeVpcEndpointAssociations",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
```

```
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConcentrators",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetAssociatedEnclaveCertificateIamRoles",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetIpamPrefixListResolverRules",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetRouteServerAssociations",
        "ec2:GetRouteServerPropagations",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayMeteringPolicyEntries",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:SearchTransitGatewayRoutes",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:DescribePullThroughCacheRules",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:DescribeRepositoryCreationTemplates",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:GetRepositoryPolicy",
        "ecr:GetSigningConfiguration",
        "ecr:ListPullTimeUpdateExclusions",
        "ecr:ListTagsForResource",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeDaemon",
        "ecs:DescribeDaemonTaskDefinition",
```

```
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:ListClusters",
        "ecs:ListDaemonTaskDefinitions",
        "ecs:ListDaemons",
        "ecs:ListServices",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeCapability",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:ListAddons",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListCapabilities",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeServerlessCaches",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeApplicationVersions",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticbeanstalk:ListTagsForResource",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
```

```
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticloadbalancing:DescribeCapacityReservation",
        "elasticloadbalancing:DescribeListenerAttributes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTrustStoreRevocations",
        "elasticloadbalancing:DescribeTrustStores",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListStudioSessionMappings",
        "elasticmapreduce:ListStudios",
        "elemental-inference:GetFeed",
        "elemental-inference:ListFeeds",
        "elemental-inference:ListTagsForResource",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:DescribeSecurityConfiguration",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListSecurityConfigurations",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:ListApplications",
        "entityresolution:GetIdMappingWorkflow",
        "entityresolution:GetIdNamespace",
        "entityresolution:GetMatchingWorkflow",
        "entityresolution:GetPolicy",
        "entityresolution:GetSchemaMapping",
        "entityresolution:ListIdMappingWorkflows",
        "entityresolution:ListIdNamespaces",
        "entityresolution:ListMatchingWorkflows",
        "entityresolution:ListSchemaMappings",
        "entityresolution:ListTagsForResource",
```

```
        "es:GetApplication",
        "es:ListApplications",
        "es:ListTags",
        "events:DescribeApiDestination",
        "events:DescribeArchive",
        "events:DescribeConnection",
        "events:DescribeEndpoint",
        "events:DescribeEventBus",
        "events:DescribeRule",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "evidently:GetSegment",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "evs:GetEnvironment",
        "evs:ListEnvironments",
        "evs:ListTagsForResource",
        "finspace:GetEnvironment",
        "finspace:ListEnvironments",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "firehose:ListTagsForDeliveryStream",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:ListExperimentTemplates",
        "fis:ListTagsForResource",
        "fis:ListTargetAccountConfigurations",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:GetResourceSet",
        "fms:ListPolicies",
        "fms:ListResourceSetResources",
        "fms:ListResourceSets",
        "fms:ListTagsForResource",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasets",
```

```
        "frauddetector:BatchGetVariable",
        "frauddetector:DescribeDetector",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetDetectors",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModelVersion",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListTagsForResource",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeS3AccessPointAttachments",
        "gamelift:DescribeAlias",
        "gamelift:DescribeBuild",
        "gamelift:DescribeContainerFleet",
        "gamelift:DescribeContainerGroupDefinition",
        "gamelift:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScalingPolicies",
        "gamelift:DescribeScript",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListContainerFleets",
        "gamelift:ListContainerGroupDefinitions",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListLocations",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "gamelift:ValidateMatchmakingRuleSet",
        "gameliftstreams:GetApplication",
        "gameliftstreams:GetStreamGroup",
```

```
        "gameliftstreams:ListApplications",
        "gameliftstreams:ListStreamGroups",
        "gameliftstreams:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeKey",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListKeys",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeCrossAccountAttachment",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCrossAccountAttachments",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "glue:DescribeIntegrations",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetCrawler",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetIntegrationResourceProperty",
        "glue:GetJob",
        "glue:GetRegistry",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetUsageProfile",
        "glue:ListCrawlers",
        "glue:ListIntegrationResourceProperties",
        "glue:ListJobs",
        "glue:ListRegistries",
        "glue:ListSchemaVersions",
        "glue:ListSchemas",
```

```
        "glue:ListTriggers",
        "glue:ListUsageProfiles",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetDeployment",
        "greengrass:ListComponentVersions",
        "greengrass:ListDeployments",
        "greengrass:ListTagsForResource",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:ListConfigs",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
        "groundstation:ListTagsForResource",
        "guardduty:DescribePublishingDestination",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetIPSet",
        "guardduty:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMembers",
        "guardduty:GetThreatEntitySet",
        "guardduty:GetThreatIntelSet",
        "guardduty:GetTrustedEntitySet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListIPSets",
        "guardduty:ListMalwareProtectionPlans",
        "guardduty:ListMembers",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatEntitySets",
        "guardduty:ListThreatIntelSets",
        "guardduty:ListTrustedEntitySets",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListTagsForResource",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
```

```
        "iam:GetLoginProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:GetWorkflow",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
```

```
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "imagebuilder:ListLifecyclePolicies",
        "imagebuilder:ListWorkflowBuildVersions",
        "imagebuilder:ListWorkflows",
        "inspector2:GetCodeSecurityIntegration",
        "inspector2:GetCodeSecurityScanConfiguration",
        "inspector2:ListCisScanConfigurations",
        "inspector2:ListCodeSecurityIntegrations",
        "inspector2:ListCodeSecurityScanConfigurations",
        "inspector2:ListFilters",
        "inspector2:ListTagsForResource",
        "inspector:DescribeAssessmentTargets",
        "inspector:DescribeAssessmentTemplates",
        "inspector:ListAssessmentTargets",
        "inspector:ListAssessmentTemplates",
        "interconnect:GetConnection",
        "interconnect:ListConnections",
        "interconnect:ListTagsForResource",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "invoicing:GetInvoiceUnit",
        "invoicing:ListInvoiceUnits",
        "invoicing:ListTagsForResource",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeBillingGroup",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCertificateProvider",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeEncryptionConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJob",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
```

```
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:GetCommand",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetPolicy",
        "iot:GetThingShadow",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:GetV2LoggingOptions",
        "iot:ListAuthorizers",
        "iot:ListBillingGroups",
        "iot:ListCACertificates",
        "iot:ListCertificateProviders",
        "iot:ListCertificates",
        "iot:ListCommands",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "iot:ListPackageVersions",
        "iot:ListPackages",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListThingGroups",
        "iot:ListThingTypes",
        "iot:ListThings",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iotanalytics:DescribeChannel",
        "iotanalytics:DescribeDataset",
        "iotanalytics:DescribeDatastore",
```

```
        "iotanalytics:DescribeLoggingOptions",
        "iotanalytics:DescribePipeline",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotanalytics:ListTagsForResource",
        "iotdeviceadvisor:GetSuiteDefinition",
        "iotdeviceadvisor:ListSuiteDefinitions",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotfleetwise:GetCampaign",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetStateTemplate",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:ListCampaigns",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListStateTemplates",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeAssetModelCompositeModel",
        "iotsitewise:DescribeAssetModelInterfaceRelationship",
        "iotsitewise:DescribeComputationModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeDataset",
        "iotsitewise:DescribeGateway",
```

```
        "iotsitewise:DescribeGatewayCapabilityConfiguration",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModelCompositeModels",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:ListComputationModels",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListDatasets",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:GetEntity",
        "iottwinmaker:GetScene",
        "iottwinmaker:GetSyncJob",
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListComponents",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListProperties",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListTagsForResource",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetPartnerAccount",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessDeviceImportTask",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
```

```
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListPartnerAccounts",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDeviceImportTasks",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "iotwireless:ListWirelessGateways",
        "ivs:GetChannel",
        "ivs:GetEncoderConfiguration",
        "ivs:GetIngestConfiguration",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetPublicKey",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStorageConfiguration",
        "ivs:GetStreamKey",
        "ivs:ListChannels",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource",
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:DescribeTopicDynamicConfiguration",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeReplicator",
        "kafka:DescribeVpcConnection",
        "kafka:GetClusterPolicy"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "WellArchitectedAgentScanningReadOnly2",
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetDirectConnectGatewayAttachment",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetSites",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:ListAttachments",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListCoreNetworkPrefixListAssociations",
        "networkmanager:ListCoreNetworks",
        "networkmanager:ListPeerings",
        "nimble:GetStudio",
        "nimble:ListStudios",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:ListTagsForResource",
        "notifications:GetEventRule",
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications:ListOrganizationalUnits",
        "notifications:ListTagsForResource",
        "nova-act:GetWorkflowDefinition",
```

```
        "nova-act:ListWorkflowDefinitions",
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListLinks",
        "oam:ListSinks",
        "oam:ListTagsForResource",
        "observabilityadmin:GetCentralizationRuleForOrganization",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:GetTelemetryEvaluationStatus",
        "observabilityadmin:GetTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:GetTelemetryPipeline",
        "observabilityadmin:GetTelemetryRule",
        "observabilityadmin:GetTelemetryRuleForOrganization",
        "observabilityadmin:ListCentralizationRulesForOrganization",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:ListTagsForResource",
        "observabilityadmin:ListTelemetryPipelines",
        "observabilityadmin:ListTelemetryRules",
        "observabilityadmin:ListTelemetryRulesForOrganization",
        "odb:GetCloudAutonomousVmCluster",
        "odb:GetCloudExadataInfrastructure",
        "odb:GetCloudVmCluster",
        "odb:GetDbNode",
        "odb:GetOdbNetwork",
        "odb:GetOdbPeeringConnection",
        "odb:ListCloudAutonomousVmClusters",
        "odb:ListCloudExadataInfrastructures",
        "odb:ListCloudVmClusters",
        "odb:ListDbNodes",
        "odb:ListDbServers",
        "odb:ListOdbNetworks",
        "odb:ListOdbPeeringConnections",
        "odb:ListTagsForResource",
        "omics:GetAnnotationStore",
        "omics:GetConfiguration",
        "omics:GetReferenceStore",
        "omics:GetRunGroup",
        "omics:GetS3AccessPolicy",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:GetWorkflowVersion",
```

```
        "omics:ListAnnotationStores",
        "omics:ListConfigurations",
        "omics:ListReferenceStores",
        "omics:ListRunGroups",
        "omics:ListSequenceStores",
        "omics:ListTagsForResource",
        "omics:ListVariantStores",
        "omics:ListWorkflowVersions",
        "omics:ListWorkflows",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
        "organizations:ListRoots",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "osis:GetPipeline",
        "osis:GetResourcePolicy",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "panorama:DescribeApplicationInstance",
        "panorama:DescribeApplicationInstanceDetails",
        "panorama:DescribePackage",
        "panorama:ListApplicationInstances",
        "panorama:ListPackages",
        "panorama:ListTagsForResource",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:GetResourcePolicy",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:ListConnectors",
```

```
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListServicePrincipalNames",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-ad:ListTemplateGroupAccessControlEntries",
        "pca-connector-ad:ListTemplates",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:ListChallengeMetadata",
        "pca-connector-scep:ListConnectors",
        "pca-connector-scep:ListTagsForResource",
        "pcs:GetCluster",
        "pcs:GetComputeNodeGroup",
        "pcs:GetQueue",
        "pcs:ListClusters",
        "pcs:ListComputeNodeGroups",
        "pcs:ListQueues",
        "pcs:ListTagsForResource",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "profile:GetCalculatedAttributeDefinition",
        "profile:GetDomain",
        "profile:GetDomainObjectType",
        "profile:GetEventStream",
        "profile:GetEventTrigger",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:GetRecommender",
        "profile:GetSegmentDefinition",
        "profile:ListCalculatedAttributeDefinitions",
        "profile:ListDomainObjectTypes",
        "profile:ListDomains",
        "profile:ListEventStreams",
        "profile:ListEventTriggers",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListRecommenders",
```

```
        "profile:ListSegmentDefinitions",
        "profile:ListTagsForResource",
        "proton:GetEnvironmentAccountConnection",
        "proton:GetEnvironmentTemplate",
        "proton:GetServiceTemplate",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentTemplates",
        "proton:ListServiceTemplates",
        "proton:ListTagsForResource",
        "qbusiness:GetApplication",
        "qbusiness:GetDataAccessor",
        "qbusiness:GetDataSource",
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetPolicy",
        "qbusiness:GetRetriever",
        "qbusiness:GetWebExperience",
        "qbusiness:ListApplications",
        "qbusiness:ListDataAccessors",
        "qbusiness:ListDataSources",
        "qbusiness:ListIndices",
        "qbusiness:ListPlugins",
        "qbusiness:ListRetrievers",
        "qbusiness:ListTagsForResource",
        "qbusiness:ListWebExperiences",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListTagsForResource",
        "quicksight:DescribeActionConnector",
        "quicksight:DescribeActionConnectorPermissions",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeCustomPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeFolder",
        "quicksight:DescribeFolderPermissions",
        "quicksight:DescribeRefreshSchedule",
        "quicksight:DescribeTemplate",
```

```
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:DescribeTopic",
        "quicksight:DescribeVPCConnection",
        "quicksight:ListActionConnectors",
        "quicksight:ListAnalyses",
        "quicksight:ListCustomPermissions",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListFolders",
        "quicksight:ListRefreshSchedules",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "quicksight:ListTopics",
        "quicksight:ListVPCConnections",
        "ram:GetPermission",
        "ram:GetResourceShares",
        "ram:ListPermissionVersions",
        "ram:ListPermissions",
        "rbin:GetRule",
        "rbin:ListRules",
        "rbin:ListTagsForResource",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBProxyTargetGroups",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeIntegrations",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
```

```
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterDbRevisions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeIntegrations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeTags",
        "redshift:GetResourcePolicy",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetRoute",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:DescribeCollection",
        "rekognition:DescribeProjects",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListCollections",
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:GetPolicy",
        "resiliencehub:GetService",
        "resiliencehub:GetSystem",
        "resiliencehub:GetUserJourney",
        "resiliencehub:ListAppVersionResourceMappings",
```

```
        "resiliencehub:ListAppVersions",
        "resiliencehub:ListApps",
        "resiliencehub:ListAssertions",
        "resiliencehub:ListInputSources",
        "resiliencehub:ListPolicies",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListServiceFunctions",
        "resiliencehub:ListServices",
        "resiliencehub:ListSystems",
        "resiliencehub:ListTagsForResource",
        "resiliencehub:ListUserJourneys",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListViews",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTagSyncTask",
        "resource-groups:GetTags",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "resource-groups:ListTagSyncTasks",
        "robomaker:DescribeFleet",
        "robomaker:DescribeRobot",
        "robomaker:DescribeRobotApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:ListFleets",
        "robomaker:ListRobotApplications",
        "robomaker:ListRobots",
        "robomaker:ListSimulationApplications",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
```

```
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53-recovery-readiness:ListTagsForResources",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListCidrBlocks",
        "route53:ListCidrCollections",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListQueryLoggingConfigs",
        "route53:ListTagsForResource",
        "route53globalresolver:GetAccessSource",
        "route53globalresolver:GetDNSView",
        "route53globalresolver:GetFirewallDomainList",
        "route53globalresolver:GetFirewallRule",
        "route53globalresolver:GetGlobalResolver",
        "route53globalresolver:GetHostedZoneAssociation",
        "route53globalresolver:ListAccessSources",
        "route53globalresolver:ListAccessTokens",
        "route53globalresolver:ListDNSViews",
        "route53globalresolver:ListFirewallDomainLists",
        "route53globalresolver:ListFirewallRules",
        "route53globalresolver:ListGlobalResolvers",
        "route53globalresolver:ListHostedZoneAssociations",
        "route53globalresolver:ListTagsForResource",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
```

```
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetOutpostResolver",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListOutpostResolvers",
        "route53resolver:ListResolverConfigs",
        "route53resolver:ListResolverDnssecConfigs",
        "route53resolver:ListResolverEndpointIpAddresses",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRuleAssociations",
        "route53resolver:ListResolverRules",
        "route53resolver:ListTagsForResource",
        "rtbfabric:GetCertificateAssociation",
        "rtbfabric:GetInboundExternalLink",
        "rtbfabric:GetLink",
        "rtbfabric:GetLinkRoutingRule",
        "rtbfabric:GetOutboundExternalLink",
        "rtbfabric:GetRequesterGateway",
        "rtbfabric:GetResponderGateway",
        "rtbfabric:ListCertificateAssociations",
        "rtbfabric:ListLinkRoutingRules",
        "rtbfabric:ListLinks",
        "rtbfabric:ListRequesterGateways",
        "rtbfabric:ListResponderGateways",
        "rtbfabric:ListTagsForResource",
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetAppMonitor",
        "rum:GetResourcePolicy",
        "rum:ListAppMonitors",
        "rum:ListRumMetricsDestinations",
        "rum:ListTagsForResource",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
```

```
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListRegionalBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointConfigurationForObjectLambda",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetObjectAcl",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsInstances",
```

```
        "s3:ListAccessGrantsLocations",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3:ListTagsForResource",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
        "s3express:GetAccessPointScope",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetInventoryConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:GetMetricsConfiguration",
        "s3express:ListAccessPointsForDirectoryBuckets",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:ListTagsForResource",
        "s3files:GetAccessPoint",
        "s3files:GetFileSystem",
        "s3files:GetFileSystemPolicy",
        "s3files:GetMountTarget",
        "s3files:GetSynchronizationConfiguration",
        "s3files:ListAccessPoints",
        "s3files:ListFileSystems",
        "s3files:ListMountTargets",
        "s3files:ListTagsForResource",
        "s3tables:GetNamespace",
        "s3tables:GetTable",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketMetricsConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableBucketReplication",
        "s3tables:GetTableBucketStorageClass",
        "s3tables:GetTableMaintenanceConfiguration",
        "s3tables:GetTablePolicy",
        "s3tables:GetTableStorageClass",
        "s3tables:ListNamespaces",
        "s3tables:ListTableBuckets",
        "s3tables:ListTables",
        "s3tables:ListTagsForResource",
```

```
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:ListIndexes",
        "s3vectors:ListTagsForResource",
        "s3vectors:ListVectorBuckets",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribePartnerApp",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeStudioLifecycleConfig",
        "sagemaker:DescribeUserProfile",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListClusters",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpoints",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceComponents",
```

```
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCardVersions",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListPartnerApps",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSpaces",
        "sagemaker:ListStudioLifecycleConfigs",
        "sagemaker:ListTags",
        "sagemaker:ListUserProfiles",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemaVersions",
        "schemas:ListSchemas",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "securityagent:BatchGetAgentSpaces",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetTargetDomains",
        "securityagent:GetApplication",
        "securityagent:ListAgentSpaces",
        "securityagent:ListApplications",
        "securityagent:ListIntegratedResources",
        "securityagent:ListPentests",
        "securityagent:ListTagsForResource",
        "securityagent:ListTargetDomains",
```

```
        "securityhub:BatchGetAutomationRules",
        "securityhub:BatchGetSecurityControls",
        "securityhub:DescribeHub",
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeSecurityHubV2",
        "securityhub:DescribeStandardsControls",
        "securityhub:GetAggregatorV2",
        "securityhub:GetAutomationRuleV2",
        "securityhub:GetConfigurationPolicy",
        "securityhub:GetConfigurationPolicyAssociation",
        "securityhub:GetConnectorV2",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindingAggregator",
        "securityhub:GetInsights",
        "securityhub:ListAggregatorsV2",
        "securityhub:ListAutomationRules",
        "securityhub:ListAutomationRulesV2",
        "securityhub:ListConfigurationPolicies",
        "securityhub:ListConfigurationPolicyAssociations",
        "securityhub:ListConnectorsV2",
        "securityhub:ListEnabledProductsForImport",
        "securityhub:ListFindingAggregators",
        "securityhub:ListOrganizationAdminAccounts",
        "securityhub:ListSecurityControlDefinitions",
        "securityhub:ListTagsForResource",
        "securitylake:GetSubscriber",
        "securitylake:ListDataLakeExceptions",
        "securitylake:ListDataLakes",
        "securitylake:ListLogSources",
        "securitylake:ListSubscribers",
        "securitylake:ListTagsForResource",
        "servicecatalog:DescribeConstraint",
        "servicecatalog:DescribePortfolio",
        "servicecatalog:DescribePortfolioShares",
        "servicecatalog:DescribeServiceAction",
        "servicecatalog:DescribeTagOption",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListApplications",
        "servicecatalog:ListAssociatedAttributeGroups",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:ListConstraintsForPortfolio",
        "servicecatalog:ListPortfolios",
```

```
        "servicecatalog:ListPortfoliosForProduct",
        "servicecatalog:ListPrincipalsForPortfolio",
        "servicecatalog:ListResourcesForTagOption",
        "servicecatalog:ListServiceActions",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:ListTagOptions",
        "servicecatalog:ListTagsForResource",
        "ses:DescribeConfigurationSet",
        "ses:GetAddonInstance",
        "ses:GetAddonSubscription",
        "ses:GetAddressList",
        "ses:GetArchive",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetCustomVerificationEmailTemplate",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailIdentity",
        "ses:GetEmailTemplate",
        "ses:GetIngressPoint",
        "ses:GetMultiRegionEndpoint",
        "ses:GetRelay",
        "ses:GetRuleSet",
        "ses:GetTemplate",
        "ses:GetTenant",
        "ses:GetTrafficPolicy",
        "ses:ListAddonInstances",
        "ses:ListAddonSubscriptions",
        "ses:ListAddressLists",
        "ses:ListArchives",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListCustomVerificationEmailTemplates",
        "ses:ListDedicatedIpPools",
        "ses:ListEmailIdentities",
        "ses:ListEmailTemplates",
        "ses:ListIngressPoints",
        "ses:ListMultiRegionEndpoints",
        "ses:ListRelays",
        "ses:ListRuleSets",
        "ses:ListTagsForResource",
        "ses:ListTemplates",
        "ses:ListTenantResources",
```

```
        "ses:ListTenants",
        "ses:ListTrafficPolicies",
        "shield:DescribeDRTAccess",
        "shield:DescribeEmergencyContactSettings",
        "shield:DescribeProtection",
        "shield:DescribeProtectionGroup",
        "shield:DescribeSubscription",
        "shield:ListProtectionGroups",
        "shield:ListProtections",
        "shield:ListTagsForResource",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningProfiles",
        "simspaceweaver:DescribeSimulation",
        "simspaceweaver:ListSimulations",
        "sms-voice:DescribeConfigurationSets",
        "sms-voice:DescribeKeywords",
        "sms-voice:DescribeOptOutLists",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeProtectConfigurations",
        "sms-voice:DescribeSenderIds",
        "sms-voice:GetProtectConfigurationCountryRuleSet",
        "sms-voice:GetResourcePolicy",
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "sns:GetDataProtectionPolicy",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:ListQueues",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:GetRotation",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListRotations",
        "ssm-contacts:ListTagsForResource",
        "ssm-guiconnect:GetConnectionRecordingPreferences",
```

```
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-sap:GetApplication",
        "ssm-sap:ListApplications",
        "ssm-sap:ListTagsForResource",
        "ssm:DescribeAssociation",
        "ssm:DescribeDocument",
        "ssm:DescribeMaintenanceWindowTargets",
        "ssm:DescribeMaintenanceWindowTasks",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeParameters",
        "ssm:DescribePatchBaselines",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetMaintenanceWindow",
        "ssm:GetMaintenanceWindowTask",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "sso-directory:DescribeGroup",
        "sso-directory:SearchGroups",
        "sso:DescribeApplication",
        "sso:DescribeApplicationAssignment",
        "sso:DescribeInstance",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetManagedApplicationInstance",
        "sso:GetPermissionsBoundaryForPermissionSet",
        "sso:ListAccountAssignments",
        "sso:ListApplicationAssignments",
        "sso:ListApplications",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListInstances",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
```

```
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
        "states:DescribeStateMachineAlias",
        "states:ListActivities",
        "states:ListStateMachineAliases",
        "states:ListStateMachineVersions",
        "states:ListStateMachines",
        "states:ListTagsForResource",
        "sts:GetCallerIdentity",
        "supportapp:GetAccountAlias",
        "supportapp:ListSlackChannelConfigurations",
        "supportapp:ListSlackWorkspaceConfigurations",
        "synthetics:DescribeCanaries",
        "synthetics:GetCanary",
        "synthetics:GetGroup",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "thinclient:GetEnvironment",
        "thinclient:ListEnvironments",
        "thinclient:ListTagsForResource",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:ListTagsForResource",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeScheduledQuery",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListScheduledQueries",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWebApp",
        "transfer:DescribeWebAppCustomization",
```

```
        "transfer:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListUsers",
        "transfer:ListWebApps",
        "transfer:ListWorkflows",
        "trustedadvisor:GetRecommendation",
        "trustedadvisor:ListChecks",
        "trustedadvisor:ListRecommendationResources",
        "trustedadvisor:ListRecommendations",
        "trustedadvisor:ListRecommendationsForResource",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyStoreAlias",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicies",
        "verifiedpermissions:ListPolicyStoreAliases",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "verifiedpermissions:ListTagsForResource",
        "voiceid:DescribeDomain",
        "voiceid:ListDomains",
        "voiceid:ListTagsForResource",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetDomainVerification",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourceConfiguration",
        "vpc-lattice:GetResourceGateway",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkResourceAssociation",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListDomainVerifications",
        "vpc-lattice:ListListeners",
```

```
        "vpc-lattice:ListResourceConfigurations",
        "vpc-lattice:ListResourceGateways",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworkResourceAssociations",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "wafv2:GetIPSet",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRegexPatternSet",
        "wafv2:GetRuleGroup",
        "wafv2:GetWebACL",
        "wafv2:ListIPSets",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRegexPatternSets",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "wafv2:ListWebACLs",
        "wisdom:GetAIAgent",
        "wisdom:GetAIGuardrail",
        "wisdom:GetAIPrompt",
        "wisdom:GetAssistant",
        "wisdom:GetAssistantAssociation",
        "wisdom:GetKnowledgeBase",
        "wisdom:GetMessageTemplate",
        "wisdom:GetQuickResponse",
        "wisdom:ListAIAgentVersions",
        "wisdom:ListAIAgents",
        "wisdom:ListAIGuardrailVersions",
        "wisdom:ListAIGuardrails",
        "wisdom:ListAIPromptVersions",
        "wisdom:ListAIPrompts",
        "wisdom:ListAssistantAssociations",
        "wisdom:ListAssistants",
        "wisdom:ListKnowledgeBases",
        "wisdom:ListMessageTemplateVersions",
        "wisdom:ListMessageTemplates",
        "wisdom:ListQuickResponses",
        "workspaces-instances:GetWorkspaceInstance",
        "workspaces-instances:ListTagsForResource",
```

```
        "workspaces-instances:ListWorkspaceInstances",
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetDataProtectionSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetIpAccessSettings",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetSessionLogger",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListDataProtectionSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListIpAccessSettings",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListSessionLoggers",
        "workspaces-web:ListSessions",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListUserSettings",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspacesPools",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetIndexingRules",
        "xray:GetSamplingRules",
        "xray:GetTraceSegmentDestination",
        "xray:ListResourcePolicies",
        "xray:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "WellArchitectedAgentScanningReadOnly3",
      "Effect" : "Allow",
      "Action" : [
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurations",
        "kafka:ListReplicators",
        "kafka:ListScramSecrets",
        "kafka:ListTagsForResource",
        "kafka:ListVpcConnections",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListTagsForResource",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra-ranking:DescribeRescoreExecutionPlan",
        "kendra-ranking:ListRescoreExecutionPlans",
        "kendra-ranking:ListTagsForResource",
        "kendra:DescribeDataSource",
        "kendra:DescribeFaq",
        "kendra:DescribeIndex",
        "kendra:ListDataSources",
        "kendra:ListFaqs",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForResource",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:DescribeStreamStorageConfiguration",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
```

```
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lakeformation:DescribeLakeFormationIdentityCenterConfiguration",
        "lakeformation:DescribeResource",
        "lakeformation:GetLFTag",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListLFTags",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCapacityProvider",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionScalingConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:ListAliases",
        "lambda:ListCapacityProviders",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListFunctionUrlConfigs",
        "lambda:ListFunctions",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "launchwizard:GetDeployment",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListTagsForResource",
        "lex:DescribeBot",
```

```
        "lex:DescribeBotAlias",
        "lex:DescribeBotReplica",
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
        "lex:GetBotAlias",
        "lex:ListBotAliases",
        "lex:ListBotLocales",
        "lex:ListBotReplicas",
        "lex:ListBotVersions",
        "lex:ListBots",
        "lex:ListIntents",
        "lex:ListSlotTypes",
        "lex:ListSlots",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListDistributedGrants",
        "license-manager:ListLicenses",
        "license-manager:ListTagsForResource",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDisks",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetInstance",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetInstances",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetLoadBalancers",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeAccountPolicies",
```

```
        "logs:DescribeDeliveries",
        "logs:DescribeDeliveryDestinations",
        "logs:DescribeDeliverySources",
        "logs:DescribeDestinations",
        "logs:DescribeIndexPolicies",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeResourcePolicies",
        "logs:DescribeSubscriptionFilters",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetIntegration",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:GetScheduledQuery",
        "logs:GetTransformer",
        "logs:ListIntegrations",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListScheduledQueries",
        "logs:ListSourcesForS3TableIntegration",
        "logs:ListTagsForResource",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListInferenceSchedulers",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:GetApplication",
        "m2:GetDeployment",
        "m2:GetEnvironment",
        "m2:ListApplications",
        "m2:ListDeployments",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "macie2:GetAllowList",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsFilter",
        "macie2:GetMacieSession",
        "macie2:ListAllowLists",
        "macie2:ListAutomatedDiscoveryAccounts",
```

```
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindingsFilters",
        "managedblockchain:GetAccessor",
        "managedblockchain:ListAccessors",
        "mediaconnect:DescribeBridge",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeGateway",
        "mediaconnect:GetRouterInput",
        "mediaconnect:GetRouterNetworkInterface",
        "mediaconnect:GetRouterOutput",
        "mediaconnect:ListBridges",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGateways",
        "mediaconnect:ListRouterInputs",
        "mediaconnect:ListRouterNetworkInterfaces",
        "mediaconnect:ListRouterOutputs",
        "mediaconnect:ListTagsForResource",
        "medialive:DescribeChannelPlacementGroup",
        "medialive:DescribeCluster",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeNetwork",
        "medialive:DescribeSdiSource",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:ListChannelPlacementGroups",
        "medialive:ListCloudWatchAlarmTemplateGroups",
        "medialive:ListCloudWatchAlarmTemplates",
        "medialive:ListClusters",
        "medialive:ListEventBridgeRuleTemplateGroups",
        "medialive:ListEventBridgeRuleTemplates",
        "medialive:ListMultiplexPrograms",
        "medialive:ListMultiplexes",
        "medialive:ListNetworks",
        "medialive:ListSdiSources",
        "medialive:ListSignalMaps",
        "medialive:ListTagsForResource",
        "mediapackage-vod:DescribeAsset",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListAssets",
```

```
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage:DescribeChannel",
        "mediapackage:DescribeOriginEndpoint",
        "mediapackage:ListChannels",
        "mediapackage:ListOriginEndpoints",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediatailor:DescribeChannel",
        "mediatailor:DescribeLiveSource",
        "mediatailor:DescribeSourceLocation",
        "mediatailor:DescribeVodSource",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListChannels",
        "mediatailor:ListLiveSources",
        "mediatailor:ListPlaybackConfigurations",
        "mediatailor:ListSourceLocations",
        "mediatailor:ListVodSources",
        "medical-imaging:GetDatastore",
        "medical-imaging:ListDatastores",
        "medical-imaging:ListTagsForResource",
        "memorydb:DescribeACLs",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeMultiRegionClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListTags",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:ListTemplates",
        "mpa:GetApprovalTeam",
        "mpa:GetIdentitySource",
        "mpa:ListApprovalTeams",
        "mpa:ListIdentitySources",
        "mpa:ListTagsForResource",
        "mq:DescribeBroker",
        "mq:DescribeConfiguration",
        "mq:DescribeSharedResources",
        "mq:ListBrokers",
```

```
        "mq:ListConfigurations",
        "mq:ListTags",
        "neptune-graph:GetGraph",
        "neptune-graph:GetGraphSnapshot",
        "neptune-graph:GetPrivateGraphEndpoint",
        "neptune-graph:ListGraphSnapshots",
        "neptune-graph:ListGraphs",
        "neptune-graph:ListPrivateGraphEndpoints",
        "neptune-graph:ListTagsForResource",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:DescribeVpcEndpointAssociation",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTLSInspectionConfigurations",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListVpcEndpointAssociations",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSWellArchitectedDiscoveryServiceRolePolicy

Deskripsi: Memungkinkan WellArchitected untuk mengakses AWS layanan dan sumber daya yang terkait dengan WellArchitected sumber daya atas nama pelanggan.

`AWSWellArchitectedDiscoveryServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 26 April 2023, 18:36 UTC
- Waktu teredit: 26 April 2023, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedDiscoveryServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeChecks",
        "trustedadvisor:DescribeCheckItems"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "resource-groups:ListGroupResources",
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:GetApplication",
        "servicecatalog:CreateAttributeGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup"
      ],
      "Resource" : [
        "arn:*:servicecatalog:*:*:/applications/*",
        "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:UpdateAttributeGroup",
        "servicecatalog:DeleteAttributeGroup"
      ],
      "Resource" : [
```

```
        "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSWellArchitectedOrganizationsServiceRolePolicy

Deskripsi: Memungkinkan Well-Architected untuk mengakses Organisasi atas nama Anda.

`AWSWellArchitectedOrganizationsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 23 Juni 2022, 17:15 UTC
- Waktu teredit: 25 Juli 2022, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSWickrFullAccess

Deskripsi: Kebijakan ini memberikan izin administratif penuh ke layanan Wickr, termasuk fungsi administratif Wickr di bawah. Konsol Manajemen AWS

`AWSWickrFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSWickrFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2022, 20:36 UTC
- Waktu teredit: 27 November 2022, 20.36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWickrFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "wickr:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSXrayCrossAccountSharingConfiguration

Deskripsi: Menyediakan kemampuan untuk mengelola tautan Pengelola Akses Observabilitas dan membuat berbagi jejak X-Ray

`AWSXrayCrossAccountSharingConfiguration`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSXrayCrossAccountSharingConfiguration` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2022, 13:46 UTC
- Waktu teredit: 27 November 2022 13.46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayCrossAccountSharingConfiguration`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:CreateLink",
        "oam:UpdateLink"
      ],
      "Resource" : [
        "arn:aws:oam:*:*:link/*",
        "arn:aws:oam:*:*:sink/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSXRayDaemonWriteAccess

Deskripsi: Iz AWS X-Ray inkan Daemon untuk menyampaikan data segmen jejak mentah ke API layanan dan mengambil data sampling (aturan, target, dll.) untuk digunakan oleh X-Ray SDK.

`AWSXRayDaemonWriteAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSXRayDaemonWriteAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Agustus 2018, 23:00 UTC
- Waktu teredit: 13 Februari 2024, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXRayDaemonWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSXrayFullAccess

Deskripsi: kebijakan AWS X-Ray terkelola akses penuh

`AWSXrayFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSXrayFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2016, 18:30 UTC
- Waktu teredit: 11 April 2024, 17.07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXrayFullAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "xray:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSXrayReadOnlyAccess

Deskripsi: kebijakan AWS X-Ray terkelola hanya baca

`AWSXrayReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSXrayReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2016, 18:27 UTC
- Waktu teredit: 14 Februari 2024, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXrayReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries",
        "xray:BatchGetTraces",
        "xray:BatchGetTraceSummaryById",
        "xray:GetDistinctTraceGraphs",
        "xray:GetServiceGraph",
        "xray:GetTraceGraph",
        "xray:GetTraceSummaries",
        "xray:GetGroups",
        "xray:GetGroup",
        "xray:ListTagsForResource",
        "xray:ListResourcePolicies",
        "xray:GetTimeSeriesServiceStatistics",
        "xray:GetInsightSummaries",
        "xray:GetInsight",
        "xray:GetInsightEvents",
        "xray:GetInsightImpactGraph"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSXrayWriteOnlyAccess

Deskripsi: hanya AWS X-Ray menulis kebijakan terkelola

`AWSXrayWriteOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSXrayWriteOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2016, 18:19 UTC
- Waktu teredit: 28 Agustus 2018, 23:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
```

```
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSZonalAutoshiftPracticeRunSLRPolicy

Deskripsi: Menyediakan akses administratif untuk menjalankan praktik shift zona ARC, dan akses ke status CloudWatch alarm untuk memantau proses latihan.

`AWSZonalAutoshiftPracticeRunSLRPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 29 November 2023, 17:34 UTC
- Waktu teredit: 30 Juni 2025, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MonitoringPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "health:DescribeEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoshiftPracticeCheckPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:DescribeInstances",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ZonalShiftManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "arc-zonal-shift:CancelZonalShift",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:StartZonalShift",
        "arc-zonal-shift:UpdateZonalShift"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

AWSZoneGroupAccessManagementServiceRolePolicy

Deskripsi: Menyediakan akses baca-saja ke API yang diperlukan untuk mendukung pengelolaan akses grup zona untuk organisasi.

`AWSZoneGroupAccessManagementServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 01 Juli 2025, 19:07 UTC
- Waktu teredit: 01 Juli 2025, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZoneGroupAccessManagementServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

BatchServiceRolePolicy

Deskripsi: Menyediakan akses untuk layanan AWS Batch untuk mengelola sumber daya yang diperlukan, termasuk sumber daya Amazon EC2 dan Amazon ECS.

`BatchServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 10 Maret 2021, 06:55 UTC
- Waktu teredit: 05 Agustus 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBatchPolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeImages",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeLaunchTemplateVersions",
```

```
        "ec2:RequestSpotFleet",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeScalingActivities",
        "eks:DescribeCluster",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTasks",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "ecs:ListTasks",
        "ecs:DeregisterTaskDefinition",
        "ecs:TagResource",
        "ecs:ListAccountSettings",
        "logs:DescribeLogGroups",
        "iam:GetInstanceProfile",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement2",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/batch/job*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement3",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/batch/job*:log-stream:*"
    },
    {
```

```
      "Sid" : "AWSBatchPolicyStatement4",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateOrUpdateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement5",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "ecs.amazonaws.com",
            "ecs-tasks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement6",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "autoscaling.amazonaws.com",
            "ecs.amazonaws.com",
            "ecs-compute.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CancelSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "ec2:DeleteLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement9",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteLaunchConfiguration"
      ],
      "Resource" :
  "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/AWSBatch*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement10",
```

```
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:SuspendProcesses",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:TerminateInstanceInAutoScalingGroup"
      ],
      "Resource" : "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
AWSBatch*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement11",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteCluster",
        "ecs:DeregisterContainerInstance",
        "ecs:PutClusterCapacityProviders",
        "ecs:RunTask",
        "ecs:StartTask",
        "ecs:StopTask",
        "ecs:UpdateCluster"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/AWSBatch*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement12",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RunTask",
        "ecs:StartTask",
        "ecs:StopTask"
      ],
      "Resource" : "arn:aws:ecs:*:*:task-definition/*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement13",
      "Effect" : "Allow",
      "Action" : [
        "ecs:StopTask"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
```

```
    },
    {
      "Sid" : "AWSBatchPolicyStatement14",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement15",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:ec2:*:*:elastic-gpu/*",
        "arn:aws:elastic-inference:*:*:elastic-inference-accelerator/*",
        "arn:aws:resource-groups:*:*:group/*"
      ]
    },
    {
      "Sid" : "AWSBatchPolicyStatement16",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateLaunchTemplate",
            "RequestSpotFleet"
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement18",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCapacityProvider",
        "ecs:UpdateCapacityProvider",
        "ecs:DeleteCapacityProvider"
      ],
      "Resource" : "arn:aws:ecs:*:*:capacity-provider/AWSBatch*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement19",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:capacity-provider/AWSBatch*"
      ]
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

BedrockAgentCoreFullAccess

Deskripsi: Menyediakan akses penuh ke Bedrock AgentCore serta akses terbatas ke layanan terkait

`BedrockAgentCoreFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `BedrockAgentCoreFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: Juli 16, 2025, 13:37 UTC
- Waktu teredit: 03 September 2026, 22:07 UTC
- ARN: `arn:aws:iam::aws:policy/BedrockAgentCoreFullAccess`

Versi kebijakan

Versi kebijakan: v21 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "BedrockAgentCoreFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:*"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:*"
    },
    {
      "Sid" : "IAMListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "BedrockAgentCorePassRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*BedrockAgentCore*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecretsManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:bedrock-agentcore*"
    },
    {
      "Sid" : "BedrockAgentCoreKMSReadAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreKMSAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:ListGrants"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "bedrock-agentcore.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreKMSGrantsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
```

```
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "GenerateDataKey"
          ]
        },
        "StringEquals" : {
          "kms:GrantConstraintType" : "EncryptionContextSubset"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:bedrock-agentcore-gateway:arn" : "arn:aws:bedrock-
agentcore:*:*:gateway/*",
          "kms:ViaService" : [
            "bedrock-agentcore.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "BedrockAgentCorePolicyKMSGrantsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo"
          ]
        },
        "StringEquals" : {
          "kms:GrantConstraintType" : "EncryptionContextSubset"
        },
        "StringLike" : {
```

```
          "kms:EncryptionContext:aws:bedrock-agentcore-policy:policy-engine-arn" :
 "arn:aws*:bedrock-agentcore:*:*:policy-engine/*",
          "kms:ViaService" : [
            "bedrock-agentcore.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::bedrock-agentcore-gateway-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock-agentcore.amazonaws.com",
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreGatewayLambdaAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:*"
      ]
    },
    {
      "Sid" : "BedrockAgentCoreGatewayApiGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis/*/stages/*/exports/*"
      ]
    },
```

```
    {
      "Sid" : "LoggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/bedrock-agentcore/*",
        "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*",
        "arn:aws:logs:*:*:log-group:aws/spans:*"
      ]
    },
    {
      "Sid" : "ObservabilityReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:BatchGet*",
        "application-signals:Get*",
        "application-signals:List*",
        "autoscaling:Describe*",
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "oam:ListSinks",
        "rum:BatchGet*",
        "rum:Get*",
        "rum:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "xray:BatchGet*",
        "xray:Get*",
        "xray:List*",
        "xray:StartTraceRetrieval",
        "xray:CancelTraceRetrieval",
```

```
        "logs:DescribeLogGroups",
        "logs:StartLiveTail",
        "logs:StopLiveTail"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TransactionSearchXRayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSegmentDestination",
        "xray:UpdateTraceSegmentDestination",
        "xray:GetIndexingRules",
        "xray:UpdateIndexingRule"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TransactionSearchLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*",
        "arn:aws:logs:*:*:log-group:aws/spans:*"
      ]
    },
    {
      "Sid" : "TransactionSearchLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "TransactionSearchApplicationSignalsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-signals:StartDiscovery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CreateBedrockAgentCoreNetworkServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/network.bedrock-
agentcore.amazonaws.com/AWSServiceRoleForBedrockAgentCoreNetwork",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "network.bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateBedrockAgentCoreGatewayNetworkServiceLinkedRolePermissions",
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/bedrock-
agentcore.amazonaws.com/AWSServiceRoleForBedrockAgentCoreGatewayNetwork",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateBedrockAgentCoreRuntimeIdentityServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/runtime-identity.bedrock-
agentcore.amazonaws.com/AWSServiceRoleForBedrockAgentCoreRuntimeIdentity",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "runtime-identity.bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateBedrockAgentCoreRuntimeInstancesServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/runtime-instances.bedrock-
agentcore.amazonaws.com/AWSServiceRoleForBedrockAgentCoreRuntimeInstances",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "runtime-instances.bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "BedrockAgentCoreRuntimeS3WriteAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::bedrock-agentcore-runtime-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreRuntimeS3ReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreRuntimeS3ListAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "BedrockAgentCoreRuntimeECRAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeRepositories",
        "ecr:DescribeImages",
        "ecr:ListImages"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/*"
      ]
    },
    {
      "Sid" : "AgentCoreEvaluationCloudWatchLogCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/bedrock-agentcore/evaluations/*"
      ]
    },
    {
      "Sid" : "AgentCoreEvaluationCloudWatchLogCustomLogGroupCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AgentCoreEvaluationCloudWatchLogIndexAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:PutIndexPolicy",
        "logs:DescribeIndexPolicies"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws/spans",
        "arn:aws:logs:*:*:log-group:aws/spans:*"
      ]
    },
    {
      "Sid" : "AgentCoreEvaluationBedrockInvokeAccess",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:inference-profile/*"
      ]
    },
    {
      "Sid" : "AgentCoreEvaluationLambdaAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:GetFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:*"
    },
    {
      "Sid" : "AgentCoreEvaluationBedrockMantleInference",
      "Effect" : "Allow",
      "Action" : "bedrock-mantle:CreateInference",
      "Resource" : "arn:aws:bedrock-mantle:*:*:project/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AgentCoreEvaluationBedrockMantleCallWithBearerToken",
      "Effect" : "Allow",
      "Action" : "bedrock-mantle:CallWithBearerToken",
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

BedrockAgentCoreNetworkServiceRolePolicy

Deskripsi: Mengizinkan akses ke sumber daya AWS layanan lain yang diperlukan untuk menjalankan Amazon Bedrock AgentCore dalam mode VPC

`BedrockAgentCoreNetworkServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 19 September 2025, 22:04 UTC
- Waktu teredit: 19 September 2025, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BedrockAgentCoreNetworkServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateEniInAnySubnet",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:subnet/*"
    },
    {
      "Sid" : "AllowCreateEniWithSecurityGroups",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "AllowCreateEniWithBedrockManagedRequestTag",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonBedrockAgentCoreManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonBedrockAgentCoreManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowTagEniOnCreate",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "AllowManageEniWhenBedrockManaged",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonBedrockAgentCoreManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowGetSecurityGroupsForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetSecurityGroupsForVPC"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "AllowDescribeNetworkingResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

BedrockAgentCoreRuntimeIdentityServiceRolePolicy

Deskripsi: Mengizinkan akses ke sumber daya manajemen identitas dan token yang diperlukan untuk otentikasi dan otorisasi Amazon Bedrock AgentCore Runtime.

`BedrockAgentCoreRuntimeIdentityServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 11 Oktober 2025, 01:04 UTC
- Waktu teredit: 11 Oktober 2025, 01:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BedrockAgentCoreRuntimeIdentityServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : {
    "Sid" : "AllowWorkloadIdentityAccess",
    "Effect" : "Allow",
    "Action" : [
      "bedrock-agentcore:GetWorkloadAccessToken",
      "bedrock-agentcore:GetWorkloadAccessTokenForJWT",
      "bedrock-agentcore:GetWorkloadAccessTokenForUserId"
    ],
    "Resource" : [
      "arn:aws:bedrock-agentcore:*:*:workload-identity-directory/default",
      "arn:aws:bedrock-agentcore:*:*:workload-identity-directory/default/workload-
identity/*"
    ]
  }
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

BedrockAgentCoreRuntimeInstancesInstanceRolePolicy

Deskripsi: Kebijakan default untuk peran instance instans yang dikelola oleh Bedrock AgentCore Runtime Instances.

`BedrockAgentCoreRuntimeInstancesInstanceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `BedrockAgentCoreRuntimeInstancesInstanceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Agustus 2026, 13:27 UTC
- Waktu teredit: 05 Agustus 2026, 13:27 UTC

- ARN: `arn:aws:iam::aws:policy/BedrockAgentCoreRuntimeInstancesInstanceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowWritingSystemLogs",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:PutSystemLogEvents"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:capacity-provider/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

BedrockAgentCoreRuntimeInstancesOperatorRolePolicy

Deskripsi: Menyediakan akses untuk membuat dan mengelola komputasi dan sumber daya terkait untuk Instans Runtime Bedrock AgentCore

`BedrockAgentCoreRuntimeInstancesOperatorRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `BedrockAgentCoreRuntimeInstancesOperatorRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Agustus 2026, 11:27 UTC
- Waktu teredit: 06 Agustus 2026, 10:12 UTC
- ARN: `arn:aws:iam::aws:policy/BedrockAgentCoreRuntimeInstancesOperatorRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeComputeResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeNetworkInterfaces",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeEventBridgeRule",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule"
      ],
      "Resource" : "arn:*:events:*:*:rule/agentcore-lifecycle-events-*"
    },
    {
      "Sid" : "CreateVolumeForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/bedrock-agentcore:capacity-provider-id" : "false"
        }
      }
    },
    {
      "Sid" : "AttachVolumeForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:ManagedResourceOperator" : "bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateLaunchTemplateForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/bedrock-agentcore:capacity-provider-id" : "false"
        }
      }
    },
    {
      "Sid" : "ModifyLaunchTemplateForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateAutoScalingForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateAutoScalingGroup"
      ],
      "Resource" : "arn:*:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
agentcore-managed-instances-*",
      "Condition" : {
```

```
        "Null" : {
          "aws:RequestTag/bedrock-agentcore:capacity-provider-id" : "false"
        }
      }
    },
    {
      "Sid" : "UpdateAndLaunchAutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:PutLifecycleHook",
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:LaunchInstances"
      ],
      "Resource" : "arn:*:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
agentcore-managed-instances-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/bedrock-agentcore:capacity-provider-id" : "false"
        }
      }
    },
    {
      "Sid" : "NetworkingAccessForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateNetworkInterface",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "AmazonAMIsAccessForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : "amazon"
        }
      }
    },
    {
      "Sid" : "CreateFleetAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:fleet/*"
      ]
    },
    {
      "Sid" : "LaunchWithManagedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/bedrock-agentcore:capacity-provider-id" : "false"
        }
      }
    },
    {
      "Sid" : "ProvisionEC2InstancesForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:volume/*"
```

```
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/bedrock-agentcore:capacity-provider-id" : "false"
        }
      }
    },
    {
      "Sid" : "TagOnCreateManagedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateFleet",
            "CreateLaunchTemplate",
            "RunInstances",
            "CreateVolume",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "TagAfterCreateManagedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:launch-template/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "bedrock-agentcore.amazonaws.com"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "bedrock-agentcore:*"
        }
      }
    },
    {
      "Sid" : "AttachNetworkInterfaceToManagedInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventBridgeAccessForManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:*:events:*:*:rule/agentcore-lifecycle-events-*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ServiceLinkedRoleAccessForAutoScaling",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/autoscaling.amazonaws.com/
AWSServiceRoleForAutoScaling"
      ]
    },
    {
      "Sid" : "PassRoleToManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/
AmazonBedrockAgentCoreCapacityProviderDefaultInstanceRole*",
        "arn:aws:iam::*:role/service-role/
AmazonBedrockAgentCoreCapacityProviderDefaultInstanceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

Penagihan

Deskripsi: Memberikan izin untuk penagihan dan pengelolaan biaya. Ini termasuk melihat penggunaan akun dan melihat serta memodifikasi anggaran dan metode pembayaran.

`Billing`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `Billing` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan fungsi pekerjaan
- Waktu pembuatan: 10 November 2016, 17:33 UTC
- Waktu teredit: 30 Juli 2026, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/Billing`

Versi kebijakan

Versi kebijakan: v30 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:*Billing",
        "aws-portal:*PaymentMethods",
        "aws-portal:*Usage",
        "billing:CreateBillingView",
        "billing:DeleteBillingView",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
```

```
        "billing:GetBillingView",
        "billing:GetContractInformation",
        "billing:GetCredits",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "billing:PutContractInformation",
        "billing:RedeemCredits",
        "billing:GetResourcePolicy",
        "billing:ListSourceViewsForBillingView",
        "billing:ListTagsForResource",
        "billing:TagResource",
        "billing:UntagResource",
        "billing:UpdateBillingPreferences",
        "billing:UpdateBillingView",
        "billing:UpdateIAMAccessPreference",
        "budgets:CreateBudgetAction",
        "budgets:DeleteBudgetAction",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionHistories",
        "budgets:ExecuteBudgetAction",
        "budgets:ModifyBudget",
        "budgets:UpdateBudgetAction",
        "budgets:ViewBudget",
        "ce:CreateCostCategoryDefinition",
        "ce:CreateNotificationSubscription",
        "ce:CreateReport",
        "ce:DeleteCostCategoryDefinition",
        "ce:DeleteNotificationSubscription",
        "ce:DeleteReport",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetCostAndUsage",
        "ce:ListCostAllocationTags",
        "ce:ListCostCategoryDefinitions",
        "ce:ListCostCategoryResourceAssociations",
        "ce:ListTagsForResource",
        "ce:TagResource",
        "ce:UpdateCostAllocationTagsStatus",
        "ce:UpdateNotificationSubscription",
        "ce:UpdatePreferences",
        "ce:UpdateReport",
        "ce:UpdateCostCategoryDefinition",
```

```
        "ce:UntagResource",
        "ce:StartCostAllocationTagBackfill",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:GetTags",
        "ce:GetDimensionValues",
        "consolidatedbilling:GetAccountBillingRole",
        "consolidatedbilling:ListLinkedAccounts",
        "cur:DeleteReportDefinition",
        "cur:DescribeReportDefinitions",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "cur:ModifyReportDefinition",
        "cur:PutClassicReportPreferences",
        "cur:PutReportDefinition",
        "cur:ValidateReportDestination",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "freetier:PutFreeTierAlertPreference",
        "invoicing:BatchGetInvoiceProfile",
        "invoicing:CreateInvoiceUnit",
        "invoicing:DeleteInvoiceUnit",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:GetInvoiceUnit",
        "invoicing:GetInvoiceCorrection",
        "invoicing:ListInvoiceSummaries",
        "invoicing:ListInvoiceUnits",
        "invoicing:ListProcurementPortals",
        "invoicing:ListProcurementPortalSuppliers",
        "invoicing:CreateProcurementPortalPreference",
        "invoicing:GetProcurementPortalPreference",
        "invoicing:PutProcurementPortalPreference",
        "invoicing:UpdateProcurementPortalPreferenceStatus",
        "invoicing:ListProcurementPortalPreferences",
        "invoicing:DeleteProcurementPortalPreference",
        "invoicing:ListTagsForResource",
        "invoicing:ListInvoiceCorrections",
        "invoicing:StartInvoiceCorrection",
        "invoicing:PutInvoiceEmailDeliveryPreferences",
        "invoicing:SendProcurementPortalValidation",
        "invoicing:TagResource",
        "invoicing:UntagResource",
        "invoicing:UpdateInvoiceUnit",
```

```
        "invoicing:VerifyProcurementPortalValidation",
        "mapcredits:ListQuarterSpend",
        "mapcredits:ListAssociatedPrograms",
        "mapcredits:ListQuarterCredits",
        "payments:CreateFinancingApplication",
        "payments:CreatePaymentInstrument",
        "payments:DeletePaymentInstrument",
        "payments:GetFinancingApplication",
        "payments:GetFinancingLine",
        "payments:GetFinancingLineWithdrawal",
        "payments:GetFinancingOption",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListFinancingApplications",
        "payments:ListFinancingLines",
        "payments:ListFinancingLineWithdrawals",
        "payments:ListPaymentPreferences",
        "payments:ListPaymentProgramOptions",
        "payments:ListPaymentProgramStatus",
        "payments:ListTagsForResource",
        "payments:ListPaymentInstruments",
        "payments:MakePayment",
        "payments:TagResource",
        "payments:UntagResource",
        "payments:UpdateFinancingApplication",
        "payments:UpdatePaymentInstrument",
        "payments:UpdatePaymentPreferences",
        "pricing:DescribeServices",
        "purchase-orders:AddPurchaseOrder",
        "purchase-orders:DeletePurchaseOrder",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "purchase-orders:ModifyPurchaseOrders",
        "purchase-orders:TagResource",
        "purchase-orders:UntagResource",
        "purchase-orders:UpdatePurchaseOrder",
        "purchase-orders:UpdatePurchaseOrderStatus",
        "purchase-orders:ViewPurchaseOrders",
        "support:CreateCase",
        "support:AddAttachmentsToSet",
        "sustainability:GetCarbonFootprintSummary",
        "tax:BatchPutTaxRegistration",
```

```
        "tax:DeleteTaxRegistration",
        "tax:GetExemptions",
        "tax:GetTaxInheritance",
        "tax:GetTaxInterview",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
        "tax:PutTaxInheritance",
        "tax:PutTaxInterview",
        "tax:PutTaxRegistration",
        "tax:UpdateExemptions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

BudgetsServiceRolePolicy

Deskripsi: Mengizinkan Anggaran memverifikasi akses ke Tampilan Penagihan yang dibagikan di seluruh batas akun.

`BudgetsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran

- Waktu pembuatan: 30 Juli 2025, 21:07 UTC
- Waktu teredit: 30 Juli 2025, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BudgetsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billing:GetBillingViewData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CertificateManagerServiceRolePolicy

Deskripsi: Kebijakan Peran Layanan Manajer Sertifikat Amazon

`CertificateManagerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 25 Juni 2020, 17:56 UTC
- Waktu teredit: 25 Juni 2020, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ClientVPNServiceConnectionsRolePolicy

Deskripsi: Kebijakan untuk mengaktifkan VPN AWS Klien untuk mengelola koneksi titik akhir VPN Klien Anda.

`ClientVPNServiceConnectionsRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 12 Agustus 2020, 19:48 UTC
- Waktu teredit: 12 Agustus 2020 19.48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ClientVPNServiceRolePolicy

Deskripsi: Kebijakan untuk mengaktifkan VPN AWS Klien untuk mengelola titik akhir VPN Klien Anda.

`ClientVPNServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 10 Desember 2018, 21:20 UTC
- Waktu teredit: 12 Agustus 2020, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInternetGateways",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAccountAttributes",
        "ds:AuthorizeApplication",
        "ds:DescribeDirectories",
        "ds:GetDirectoryLimits",
        "ds:UnauthorizeApplication",
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "acm:GetCertificate",
        "acm:DescribeCertificate",
        "iam:GetSAMLProvider",
        "lambda:GetFunctionConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudFormationStackSetsOrgAdminServiceRolePolicy

Deskripsi: Peran Layanan untuk CloudFormation StackSets (Akun Master Organisasi)

`CloudFormationStackSetsOrgAdminServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 10 Desember 2019, 00:20 UTC
- Waktu teredit: 10 Desember 2019, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsAWSOrganizationsReadAPIs",
      "Effect" : "Allow",
```

```
      "Action" : [
        "organizations:List*",
        "organizations:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeRoleInMemberAccounts",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/stacksets-exec-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudFormationStackSetsOrgMemberServiceRolePolicy

Deskripsi: Peran Layanan untuk CloudFormation StackSets (Akun Anggota Organisasi)

`CloudFormationStackSetsOrgMemberServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 09 Desember 2019, 23:52 UTC
- Waktu teredit: 22 Juli 2026, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/stacksets-exec-role-stack-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/stacksets-exec-*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/stacksets-exec-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/AdministratorAccess"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudFrontFullAccess

Deskripsi: Menyediakan akses penuh ke CloudFront konsol ditambah kemampuan untuk membuat daftar bucket Amazon S3 melalui Konsol Manajemen AWS.

`CloudFrontFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudFrontFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu teredit: 30 Juli 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontFullAccess`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfflistbuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "cffullaccess",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudfront:*",
        "cloudfront-keyvaluestore:*",
        "iam:ListServerCertificates",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
```

```
        "wafv2:GetWebACL",
        "wafv2:CreateWebACL",
        "kinesis:ListStreams",
        "ec2:DescribeInstances",
        "elasticloadbalancing:DescribeLoadBalancers",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamPools",
        "ec2:GetIpamPoolCidrs",
        "pricingplanmanager:ListSubscriptions",
        "pricingplanmanager:CreateSubscription",
        "cloudwatch:GetMetricData",
        "freetier:GetAccountPlanState",
        "shield:ListProtections"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "cfrequestcertificate",
      "Effect" : "Allow",
      "Action" : [
        "acm:RequestCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "cloudfront.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cffdescribestream",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream"
      ],
      "Resource" : "arn:aws:kinesis:*:*:*"
    },
    {
      "Sid" : "cfflistroles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "arn:aws:iam::*:*"
```

```
    },
    {
      "Sid" : "ppmFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:ApprovePaidSubscription",
        "pricingplanmanager:AssociateResourcesToSubscription",
        "pricingplanmanager:CancelSubscription",
        "pricingplanmanager:CancelSubscriptionChange",
        "pricingplanmanager:DisassociateResourcesFromSubscription",
        "pricingplanmanager:GetSubscription",
        "pricingplanmanager:UpdateSubscription"
      ],
      "Resource" : "arn:aws:pricingplanmanager::*:subscription:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudFrontReadOnlyAccess

Deskripsi: Menyediakan akses ke informasi konfigurasi CloudFront distribusi dan daftar distribusi melalui Konsol Manajemen AWS.

`CloudFrontReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudFrontReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudfront:Describe*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudfront-keyvaluestore:Describe*",
        "cloudfront-keyvaluestore:Get*",
        "cloudfront-keyvaluestore:List*",
        "iam:ListServerCertificates",
        "route53:List*",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL",
        "ec2:DescribeIpamPools",
        "ec2:GetIpamPoolCidrs",
        "pricingplanmanager:ListSubscriptions",
        "pricingplanmanager:GetSubscription"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudHSMServiceRolePolicy

Deskripsi: Mengaktifkan akses ke AWS sumber daya yang digunakan atau dikelola oleh CloudHSM

`CloudHSMServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 06 November 2017, 19:12 UTC
- Waktu teredit: 06 November 2017, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudSearchFullAccess

Deskripsi: Menyediakan akses penuh ke layanan CloudSearch konfigurasi Amazon.

`CloudSearchFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudSearchFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC

- Waktu teredit: 06 Februari 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudSearchReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke layanan CloudSearch konfigurasi Amazon.

`CloudSearchReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudSearchReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu teredit: 06 Februari 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:Describe*",
        "cloudsearch:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudTrailEventContext

Deskripsi: Peran tertaut layanan ini memungkinkan CloudTrail untuk mendapatkan dan menambahkan tag sumber daya ke CloudTrail peristiwa pemilik sumber daya.

`CloudTrailEventContext`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 15 Mei 2025, 13:52 UTC
- Waktu teredit: 15 Mei 2025, 13:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailEventContext`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudTrailEventContextPermissionForTag",
      "Effect" : "Allow",
```

```
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeRuleCreation",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/CloudTrailEventContext*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:source" : "aws.tag"
        },
        "StringEquals" : {
          "events:creatorAccount" : "${aws:PrincipalAccount}",
          "events:detail-type" : "Tag Change on Resource",
          "events:ManagedBy" : "context.cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeRuleWrite",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/CloudTrailEventContext*",
      "Condition" : {
        "StringEquals" : {
          "events:creatorAccount" : "${aws:PrincipalAccount}",
          "events:ManagedBy" : "context.cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeRuleRead",
      "Effect" : "Allow",
      "Action" : [
```

```
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Condition" : {
        "StringEquals" : {
          "events:creatorAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:events:*:*:rule/CloudTrailEventContext*"
    },
    {
      "Sid" : "AllowEventBridgeRuleList",
      "Effect" : "Allow",
      "Action" : [
        "events:ListRules"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudTrailServiceRolePolicy

Deskripsi: Kebijakan izin untuk CloudTrail ServiceLinkedRole

`CloudTrailServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran

- Waktu pembuatan: 24 Oktober 2018, 21:21 UTC
- Waktu teredit: 27 November 2023, 01:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudTrailFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AwsOrgsDelegatedAdminAccess",
      "Effect" : "Allow",
```

```
      "Action" : "organizations:ListDelegatedAdministrators",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "cloudtrail.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DeleteTableAccess",
      "Effect" : "Allow",
      "Action" : "glue:DeleteTable",
      "Resource" : [
        "arn:*:glue:*:*:catalog",
        "arn:*:glue:*:*:database/aws:cloudtrail",
        "arn:*:glue:*:*:table/aws:cloudtrail/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DeregisterResourceAccess",
      "Effect" : "Allow",
      "Action" : "lakeformation:DeregisterResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatch-CrossAccountAccess

Deskripsi: CloudWatch Memungkinkan untuk CloudWatch-CrossAccountSharing mengambil peran dalam akun jarak jauh atas nama akun saat ini untuk menampilkan data lintas akun, lintas wilayah

`CloudWatch-CrossAccountAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 23 Juli 2019, 09:59 UTC
- Waktu teredit: 23 Juli 2019, 09:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
      ],
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchActionsEC2Access

Deskripsi: Menyediakan akses baca-saja ke CloudWatch alarm dan metrik serta metadata EC2. Menyediakan akses ke Instans Stop, Terminate, dan Reboot EC2.

`CloudWatchActionsEC2Access`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchActionsEC2Access` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Juli 2015, 00:00 UTC
- Waktu teredit: 07 Juli 2015, 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchActionsEC2Access`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchAgentAdminPolicy

Deskripsi: Izin penuh diperlukan untuk menggunakan AmazonCloudWatchAgent.

`CloudWatchAgentAdminPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchAgentAdminPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 07 Maret 2018, 00:52 UTC
- Waktu teredit: 05 Februari 2024, 20:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CWACloudWatchPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:DescribeTags",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWASSMPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchAgentServerPolicy

Deskripsi: Izin diperlukan untuk digunakan AmazonCloudWatchAgent di server

`CloudWatchAgentServerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchAgentServerPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Maret 2018, 01:06 UTC
- Waktu teredit: 06 Februari 2024, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CWACloudWatchServerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:DescribeVolumes",
        "ec2:DescribeTags",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWASSMServerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchAPIKeyAccess

Deskripsi: Memberikan izin untuk memanggil CloudWatch menggunakan otentikasi kunci API.

`CloudWatchAPIKeyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchAPIKeyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Mei 2026, 08:57 UTC
- Waktu teredit: 04 Juni 2026, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAPIKeyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchMetricsAPIs",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:CallWithBearerToken",
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSDecryptForCMKDatasets",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "cloudwatch.*.amazonaws.com",
          "kms:EncryptionContext:aws:cloudwatch:arn" : "arn:aws:cloudwatch:*:*:dataset/
*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchApplicationInsightsFullAccess

Deskripsi: Menyediakan akses penuh ke CloudWatch Application Insights dan dependensi yang diperlukan.

`CloudWatchApplicationInsightsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchApplicationInsightsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 November 2020, 18:44 UTC
- Waktu teredit: 25 Januari 2022, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "sqs:ListQueues",
```

```
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "autoscaling:DescribeAutoScalingGroups",
        "lambda:ListFunctions",
        "dynamodb:ListTables",
        "s3:ListAllMyBuckets",
        "sns:ListTopics",
        "states:ListStateMachines",
        "apigateway:GET",
        "ecs:ListClusters",
        "ecs:DescribeTaskDefinition",
        "ecs:ListServices",
        "ecs:ListTasks",
        "eks:ListClusters",
        "eks:ListNodegroups",
        "fsx:DescribeFileSystems",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "application-insights.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchApplicationInsightsReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Appl CloudWatch ication Insights.

`CloudWatchApplicationInsightsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchApplicationInsightsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 November 2020, 18:48 UTC
- Waktu teredit: 24 November 2020, 18.48 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:Describe*",
```

```
        "applicationinsights:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudwatchApplicationInsightsServiceLinkedRolePolicy

Deskripsi: Kebijakan Peran Terkait Layanan Wawasan Aplikasi Cloudwatch

`CloudwatchApplicationInsightsServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 01 Desember 2018, 16:22 UTC
- Waktu teredit: 25 Juli 2024, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v25 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:PutAnomalyDetector",
        "cloudwatch:DeleteAnomalyDetector",
        "cloudwatch:DescribeAnomalyDetectors"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
```

```
      "Action" : [
        "events:DescribeRule"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudFormation",
      "Effect" : "Allow",
      "Action" : [
        "cloudFormation:CreateStack",
        "cloudFormation:UpdateStack",
        "cloudFormation:DeleteStack",
        "cloudFormation:DescribeStackResources",
        "cloudFormation:UpdateTerminationProtection"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/ApplicationInsights-*"
      ]
    },
    {
      "Sid" : "CloudFormationStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudFormation:DescribeStacks",
        "cloudFormation:ListStackResources",
        "cloudFormation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Tag",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "ResourceGroups",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ApplicationInsightsResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup"
      ],
      "Resource" : [
        "arn:aws:resource-groups:*:*:group/ApplicationInsights-*"
      ]
    },
    {
      "Sid" : "ElasticLoadBalancing",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "SSMParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-ApplicationInsights-*"
    },
    {
      "Sid" : "SSMAssociation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:document/AmazonCloudWatch-ManageAgent"
      ]
    },
    {
      "Sid" : "SSMOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:CreateOpsItem",
        "ssm:DescribeOpsItems",
        "ssm:UpdateOpsItem",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "SSMTags",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
      "Sid" : "SSMGetCommandInvocation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommandInvocations",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMSendCommand",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AWSEC2-CheckPerformanceCounterSets",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:document/AWSEC2-DetectWorkload",
        "arn:aws:ssm:*:*:document/AmazonCloudWatch-ManageAgent"
      ]
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeNatGateways"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "RDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Lambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions",
        "lambda:GetFunctionConfiguration",
        "lambda:ListEventSourceMappings"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EventBridgeManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AmazonCloudWatch-ApplicationInsights-*"
      ]
    },
    {
      "Sid" : "XRay",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetServiceGraph",
```

```
        "xray:GetTraceSummaries",
        "xray:GetTimeSeriesServiceStatistics",
        "xray:GetTraceGraph"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DynamoDB",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeTimeToLive"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ApplicationAutoscaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetMetricsConfiguration",
        "s3:GetReplicationConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "States",
      "Effect" : "Allow",
      "Action" : [
        "states:ListStateMachines",
        "states:DescribeExecution",
        "states:DescribeStateMachine",
        "states:GetExecutionHistory"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "APIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTasks",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "ecs:ListTasks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ECSCluster",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecs:UpdateClusterSettings"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "EKS",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodegroup",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListNodegroups",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:GetSMSAttributes",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SQS",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ListQueues"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsDeleteSubscriptionFilter",
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteSubscriptionFilter"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Sid" : "CloudWatchLogsCreateSubscriptionFilter",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutSubscriptionFilter"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*",
        "arn:aws:logs:*:*:destination:AmazonCloudWatch-ApplicationInsights-
LogIngestionDestination*"
      ]
    },
    {
      "Sid" : "EFS",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFileSystems"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Route53",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:GetHealthCheck",
        "route53:ListHostedZones",
        "route53:ListHealthChecks",
        "route53:ListQueryLoggingConfigs"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Route53Resolver",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetFirewallRuleGroupAssociation"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchApplicationSignalsFullAccess

Deskripsi: Menyediakan akses penuh ke layanan Sinyal CloudWatch Aplikasi dan akses cakupan ke dependensi yang diperlukan untuk menggunakan dan mengoperasikan layanan ini.

`CloudWatchApplicationSignalsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchApplicationSignalsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Juni 2024, 22:50 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : "application-signals:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsAlarmsPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:DescribeAlarms",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsMetricsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetQueryResults",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSyntheticsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:GetCanaryRuns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsRumPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rum:BatchCreateRumMetricDefinitions",
        "rum:BatchDeleteRumMetricDefinitions",
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:PutRumMetricsDestination",
        "rum:UpdateRumMetricDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayTracePermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSummaries"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:StartTraceRetrieval",
        "xray:ListRetrievedTraces",
        "xray:BatchGetTraces",
        "xray:GetTraceSegmentDestination"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-signals.cloudwatch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsPutMetricAlarmPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricAlarm",
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:SLO-AttainmentGoalAlarm-*",
        "arn:aws:cloudwatch:*:*:alarm:SLO-WarningAlarm-*",
        "arn:aws:cloudwatch:*:*:alarm:SLI-HealthAlarm-*"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
      "Effect" : "Allow",
```

```
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSnsWritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:cloudwatch-application-signals-*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSnsReadPermissions",
      "Effect" : "Allow",
      "Action" : "sns:ListTopics",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:GetChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListChannels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
```

```
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerCreateIndexPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "resource-explorer-2:CreateIndex"
      ],
      "Resource" : "arn:aws:resource-explorer-2:*:*:index/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMAttachedLinksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMListSinksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListSinks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchApplicationSignalsReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke layanan Sinyal CloudWatch Aplikasi dan akses cakupan ke dependensi yang diperlukan untuk menggunakan layanan ini

`CloudWatchApplicationSignalsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchApplicationSignalsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Juni 2024, 22:48 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServiceDependencies",
        "application-signals:ListServiceDependents",
        "application-signals:ListServiceOperations",
        "application-signals:ListServices",
        "application-signals:ListTagsForResource",
        "application-signals:ListServiceStates",
        "application-signals:ListAuditFindings",
```

```
        "application-signals:ListGroupingAttributeDefinitions",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListEntityEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetQueryResults",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsAlarmsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsMetricsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSyntheticsReadPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:GetCanaryRuns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsRumReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayTracePermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:StartTraceRetrieval",
        "xray:ListRetrievedTraces",
        "xray:BatchGetTraces",
        "xray:GetTraceSegmentDestination"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-signals.cloudwatch.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListChannels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
      "Resource" : [
```

```
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMAttachedLinksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMListSinksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListSinks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchApplicationSignalsServiceRolePolicy

Deskripsi: Kebijakan memberikan izin kepada Sin CloudWatch yal Aplikasi untuk mengumpulkan data pemantauan dan penandaan dari AWS layanan terkait lainnya.

`CloudWatchApplicationSignalsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 09 November 2023, 18:09 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "XRayPermission",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetServiceGraph"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "CWLogsPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/appsignals/*:*",
        "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CWListMetricsPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CWGetMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "TagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ApplicationSignalsPermission",
      "Effect" : "Allow",
      "Action" : [
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:GetServiceLevelObjective"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2AutoScalingPermission",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "ResourceExplorerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudTrailServiceLinkedChannelCreationPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
      ],
      "Resource" : [
        "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-signals/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchAutomaticDashboardsAccess

Deskripsi: Menyediakan akses ke CloudWatch non-API yang digunakan untuk menampilkan CloudWatch Dasbor Otomatis, termasuk konten objek seperti fungsi Lambda

`CloudWatchAutomaticDashboardsAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchAutomaticDashboardsAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Juli 2019, 10:01 UTC
- Waktu teredit: 07 Agustus 2026, 10:42 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "cloudfront:GetDistribution",
        "cloudfront:ListDistributions",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "elasticache:DescribeCacheClusters",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeLoadBalancers",
        "kinesis:DescribeStream",
```

```
        "kinesis:ListStreams",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
        "lambda:ListTags",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListQueues",
        "synthetics:DescribeCanariesLastRun",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchCrossAccountSharingConfiguration

Deskripsi: Menyediakan kemampuan untuk mengelola tautan Pengelola Akses Observabilitas dan menetapkan berbagi sumber daya CloudWatch

`CloudWatchCrossAccountSharingConfiguration`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchCrossAccountSharingConfiguration` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2022, 14:01 UTC
- Waktu teredit: 27 November 2022, 14:01 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchCrossAccountSharingConfiguration`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Link",
        "oam:ListLinks"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:CreateLink",
        "oam:UpdateLink"
      ],
      "Resource" : [
        "arn:aws:oam:*:*:link/*",
        "arn:aws:oam:*:*:sink/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchEventsBuiltInTargetExecutionAccess

Deskripsi: Mengizinkan target bawaan di Amazon Ev CloudWatch ents untuk melakukan tindakan EC2 atas nama Anda.

`CloudWatchEventsBuiltInTargetExecutionAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchEventsBuiltInTargetExecutionAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Januari 2016, 18:35 UTC
- Waktu teredit: 14 Januari 2016, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchEventsFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon CloudWatch Events.

`CloudWatchEventsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchEventsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Januari 2016, 18:37 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "apidestinations.events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "schemas.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecretsManagerAccessForApiDestinations",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
```

```
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!*"
    },
    {
      "Sid" : "IAMPassRoleForCloudWatchEvents",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS_Events_Invoke_Targets"
    },
    {
      "Sid" : "IAMPassRoleAccessForScheduler",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchEventsInvocationAccess

Deskripsi: Mengiz CloudWatch inkan Amazon Events untuk menyampaikan peristiwa ke streaming di AWS Kinesis Streams di akun Anda.

`CloudWatchEventsInvocationAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchEventsInvocationAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Januari 2016, 18:36 UTC
- Waktu teredit: 14 Januari 2016, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsInvocationAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchEventsReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon CloudWatch Events.

`CloudWatchEventsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchEventsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Januari 2016, 18:27 UTC
- Waktu teredit: 01 Desember 2022, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DescribeEventBus",
        "events:DescribeEventSource",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:TestEventPattern",
        "events:DescribeArchive",
        "events:ListArchives",
        "events:DescribeReplay",
        "events:ListReplays",
        "events:DescribeConnection",
        "events:ListConnections",
        "events:DescribeApiDestination",
        "events:ListApiDestinations",
        "events:DescribeEndpoint",
        "events:ListEndpoints",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:ExportSchema",
        "schemas:GetCodeBindingSource",
        "schemas:GetDiscoveredSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
```

```
        "schemas:ListTagsForResource",
        "schemas:SearchSchemas",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:ListTagsForResource",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchEventsServiceRolePolicy

Deskripsi: Izinkan AWS CloudWatch untuk menjalankan tindakan atas nama Anda yang dikonfigurasi melalui alarm dan peristiwa.

`CloudWatchEventsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 17 November 2017, 00:42 UTC

- Waktu teredit: 17 November 2017, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchFullAccess

Deskripsi: Menyediakan akses penuh ke CloudWatch.

`CloudWatchFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 27 November 2022 13.23 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudwatch:*",
        "logs:*",
        "sns:*",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
```

```
        "oam:ListSinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.amazonaws.com/
AWSServiceRoleForCloudWatchEvents*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "events.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchFullAccessV2

Deskripsi: Menyediakan akses penuh ke CloudWatch.

`CloudWatchFullAccessV2`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchFullAccessV2` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Agustus 2023, 11:32 UTC
- Waktu teredit: 22 September 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccessV2`

Versi kebijakan

Versi kebijakan: v17 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:*",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribePolicies",
        "cloudwatch:*",
        "logs:*",
        "sns:CreateTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "oam:ListSinks",
        "observabilityadmin:GetCentralizationRuleForOrganization",
```

```
        "observabilityadmin:ListCentralizationRulesForOrganization",
        "observabilityadmin:CreateCentralizationRuleForOrganization",
        "observabilityadmin:UpdateCentralizationRuleForOrganization",
        "observabilityadmin:DeleteCentralizationRuleForOrganization",
        "observabilityadmin:StartTelemetryEvaluation",
        "observabilityadmin:GetTelemetryEvaluationStatus",
        "observabilityadmin:ListResourceTelemetry",
        "observabilityadmin:StopTelemetryEvaluation",
        "observabilityadmin:StartTelemetryEvaluationForOrganization",
        "observabilityadmin:GetTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:ListResourceTelemetryForOrganization",
        "observabilityadmin:StopTelemetryEvaluationForOrganization",
        "observabilityadmin:CreateTelemetryRule",
        "observabilityadmin:GetTelemetryRule",
        "observabilityadmin:ListTelemetryRules",
        "observabilityadmin:UpdateTelemetryRule",
        "observabilityadmin:DeleteTelemetryRule",
        "observabilityadmin:CreateTelemetryRuleForOrganization",
        "observabilityadmin:GetTelemetryRuleForOrganization",
        "observabilityadmin:ListTelemetryRulesForOrganization",
        "observabilityadmin:UpdateTelemetryRuleForOrganization",
        "observabilityadmin:DeleteTelemetryRuleForOrganization",
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:StartTelemetryEnrichment",
        "observabilityadmin:StopTelemetryEnrichment",
        "observabilityadmin:TagResource",
        "observabilityadmin:UntagResource",
        "observabilityadmin:ListTagsForResource",
        "observabilityadmin:CreateTelemetryPipeline",
        "observabilityadmin:GetTelemetryPipeline",
        "observabilityadmin:UpdateTelemetryPipeline",
        "observabilityadmin:DeleteTelemetryPipeline",
        "observabilityadmin:ListTelemetryPipelines",
        "observabilityadmin:TestTelemetryPipeline",
        "observabilityadmin:ValidateTelemetryPipelineConfiguration",
        "observabilityadmin:CreateS3TableIntegration",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:DeleteS3TableIntegration",
        "observabilityadmin:CreateDatasetIntegration",
        "observabilityadmin:GetDatasetIntegration",
        "observabilityadmin:ListDatasetIntegrations",
        "observabilityadmin:UpdateDatasetIntegration",
        "observabilityadmin:DeleteDatasetIntegration",
```

```
        "rum:*",
        "synthetics:*",
        "xray:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventsServicePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.amazonaws.com/
AWSServiceRoleForCloudWatchEvents*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:GetChannel"
```

```
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListChannels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
    },
    {
      "Sid" : "CloudWatchResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    },
```

```
    {
      "Sid" : "CloudWatchResourceExplorerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchResourceExplorerCreateIndexPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:CreateIndex"
      ],
      "Resource" : "arn:aws:resource-explorer-2:*:*:index/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "logs.amazonaws.com"
        },
        "ArnLike" : {
          "iam:AssociatedResourceArn" :
 "arn:aws:observabilityadmin:*:*:s3tableintegration/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : [
            "logs.amazonaws.com",
            "telemetry-pipelines.observabilityadmin.amazonaws.com"
          ]
        },
        "ArnLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:observabilityadmin:*:*:telemetry-
pipeline/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:CreateTableBucket",
        "s3tables:PutTableBucketEncryption"
      ],
      "Resource" : "arn:aws:s3tables:*:*:bucket/aws-cloudwatch",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "observabilityadmin.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:PutTableBucketPolicy"
      ],
      "Resource" : "arn:aws:s3tables:*:*:bucket/aws-cloudwatch"
    },
    {
      "Sid" : "LogAlarmScheduledQueryPassRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "logs.amazonaws.com"
        },
        "ArnLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:logs:*:*:scheduled-query:*"
        }
      }
```

```
    },
    {
      "Sid" : "LogAlarmLogLinesPassRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cloudwatch.amazonaws.com"
        },
        "ArnLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:cloudwatch:*:*:alarm:*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchInternetMonitorFullAccess

Deskripsi: Menyediakan akses penuh ke tindakan untuk bekerja dengan Amazon CloudWatch Internet Monitor. Juga menyediakan akses ke layanan lain, seperti Amazon CloudWatch, Amazon EC2, Amazon, Amazon CloudFront WorkSpaces, dan Elastic Load Balancing, yang diperlukan untuk menggunakan layanan Internet Monitor untuk memantau dan menyimpan informasi tentang lalu lintas aplikasi.

`CloudWatchInternetMonitorFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchInternetMonitorFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 Oktober 2024, 21:02 UTC
- Waktu teredit: 22 Oktober 2024, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchInternetMonitorFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FullAccessActions",
      "Effect" : "Allow",
      "Action" : [
        "internetmonitor:CreateMonitor",
        "internetmonitor:DeleteMonitor",
        "internetmonitor:GetHealthEvent",
        "internetmonitor:GetInternetEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:GetQueryResults",
        "internetmonitor:GetQueryStatus",
        "internetmonitor:Link",
        "internetmonitor:ListHealthEvents",
        "internetmonitor:ListInternetEvents",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "internetmonitor:StartQuery",
        "internetmonitor:StopQuery",
        "internetmonitor:TagResource",
        "internetmonitor:UntagResource",
```

```
        "internetmonitor:UpdateMonitor"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ServiceLinkedRoleActions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/internetmonitor.amazonaws.com/
AWSServiceRoleForInternetMonitor",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "internetmonitor.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "RolePolicyActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/internetmonitor.amazonaws.com/
AWSServiceRoleForInternetMonitor",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/aws-service-role/
CloudWatchInternetMonitorServiceRolePolicy"
        }
      }
    },
    {
      "Sid" : "ReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudfront:GetDistribution",
        "cloudfront:ListDistributions",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "logs:DescribeLogGroups",
        "logs:GetQueryResults",
        "logs:StartQuery",
        "logs:StopQuery",
```

```
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchInternetMonitorReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke tindakan untuk bekerja dengan Amazon CloudWatch Internet Monitor. Juga menyediakan akses ke layanan lain di Amazon CloudWatch, termasuk kebijakan untuk mengambil informasi tentang CloudWatch metrik dan untuk mengelola kueri log, yang diperlukan untuk menggunakan layanan Internet Monitor untuk memantau dan menyimpan informasi tentang lalu lintas aplikasi.

`CloudWatchInternetMonitorReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchInternetMonitorReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 November 2024, 23:11 UTC
- Waktu teredit: 12 November 2024, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchInternetMonitorReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "internetmonitor:GetHealthEvent",
        "internetmonitor:GetInternetEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:GetQueryResults",
        "internetmonitor:GetQueryStatus",
        "internetmonitor:ListHealthEvents",
        "internetmonitor:ListInternetEvents",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "internetmonitor:StartQuery",
        "internetmonitor:StopQuery",
        "logs:DescribeLogGroups",
        "logs:GetQueryResults",
        "logs:StartQuery",
        "logs:StopQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchInternetMonitorServiceRolePolicy

Deskripsi: Mengizinkan Monitor Internet mengakses EC2, Ruang Kerja, dan CloudFront sumber daya, serta layanan lain yang diperlukan atas nama Anda.

`CloudWatchInternetMonitorServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 27 November 2022, 17:46 UTC
- Waktu teredit: 20 Juli 2023, 04:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/internet-monitor/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/internet-monitor/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/InternetMonitor"
        }
      },
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchLambdaApplicationSignalsExecutionRolePolicy

Deskripsi: Menyediakan akses tulis ke X-Ray dan grup log Sinyal CloudWatch Aplikasi.

`CloudWatchLambdaApplicationSignalsExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchLambdaApplicationSignalsExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 Oktober 2024, 19:09 UTC
- Waktu teredit: 16 Oktober 2024, 19:09 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLambdaApplicationSignalsExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsXrayWritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogGroupWritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchLambdaInsightsExecutionRolePolicy

Deskripsi: Kebijakan diperlukan untuk Ekstensi Lambda Insights

`CloudWatchLambdaInsightsExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchLambdaInsightsExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Oktober 2020, 19:27 UTC
- Waktu teredit: 07 Oktober 2020, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda-insights:*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchLogsAPIKeyAccess

Deskripsi: Memberikan izin untuk memanggil CloudWatch Log menggunakan otentikasi kunci API.

`CloudWatchLogsAPIKeyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchLogsAPIKeyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: Februari 20, 2026, 19:42 UTC
- Waktu teredit: 20 Februari 2026, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsAPIKeyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LogsAPIs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CallWithBearerToken",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSAPIs",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "logs.*.amazonaws.com"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:logs:arn" : "arn:aws:logs:*:*:log-group:*"
        }
      },
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "KMSDescribeAPIs",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "logs.*.amazonaws.com"
        }
      },
      "Resource" : "arn:aws:kms:*:*:key/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchLogsCrossAccountSharingConfiguration

Deskripsi: Menyediakan kemampuan untuk mengelola tautan Pengelola Akses Observabilitas dan membuat berbagi sumber daya CloudWatch Log

`CloudWatchLogsCrossAccountSharingConfiguration`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchLogsCrossAccountSharingConfiguration` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2022, 13:55 UTC
- Waktu teredit: 27 November 2022 13.55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:CreateLink",
        "oam:UpdateLink"
      ],
      "Resource" : [
        "arn:aws:oam:*:*:link/*",
        "arn:aws:oam:*:*:sink/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchLogsFullAccess

Deskripsi: Menyediakan akses penuh ke CloudWatch Log

`CloudWatchLogsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchLogsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsFullAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:*",
        "cloudwatch:GenerateQuery",
```

```
        "cloudwatch:GenerateQueryResultsSummary",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:ListTelemetryPipelines"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchLogsReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke CloudWatch Log

`CloudWatchLogsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchLogsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GenerateQueryResultsSummary",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListTelemetryPipelines"
      ],
      "Resource" : "*"
    }
  ]
}
```


Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchNetworkFlowMonitorAgentPublishPolicy

Deskripsi: Anda dapat menggunakan kebijakan ini di peran IAM yang dilampirkan ke sumber instans Amazon EC2 dan Amazon EKS untuk mengirim laporan telemetri (metrik) ke titik akhir Monitor Aliran Jaringan.

`CloudWatchNetworkFlowMonitorAgentPublishPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchNetworkFlowMonitorAgentPublishPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2024, 22:51 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchNetworkFlowMonitorAgentPublishPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "networkflowmonitor:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchNetworkFlowMonitorServiceRolePolicy

Deskripsi: Anda tidak dapat melampirkan CloudWatchNetworkFlowMonitorServiceRolePolicy ke entitas IAM Anda. Kebijakan ini dilampirkan ke peran terkait layanan bernama AWSServiceRoleForNetworkFlowMonitor, yang menerbitkan hasil agregasi telemetri jaringan, yang dikumpulkan oleh agen Monitor Aliran Jaringan, ke. CloudWatch Ini juga memungkinkan layanan untuk menggunakan AWS Organisasi untuk mendapatkan informasi untuk skenario multi-akun.

`CloudWatchNetworkFlowMonitorServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 01 Desember 2024, 22:36 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkFlowMonitorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/NetworkFlowMonitor"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/*"
      ]
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy

Deskripsi: Anda tidak dapat melampirkan CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy ke entitas IAM Anda. Kebijakan ini dilampirkan ke peran terkait layanan bernama AWSServiceRoleForNetworkFlowMonitor _Topology, yang menghasilkan snapshot topologi sumber daya yang digunakan oleh Network Flow Monitor di akun Anda.

`CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 01 Desember 2024, 22:51 UTC
- Waktu teredit: 01 September 2026, 01:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TransitGatewayAndVPNStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpnConnections",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrefixListStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VPCEndpointStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "LoadBalancerStatement",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroupAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWANStatement",
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:ListCoreNetworks",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:ListAttachments",
        "networkmanager:GetVpcAttachment",
        "networkmanager:GetNetworkRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConfigRecorderCreateDelete",
      "Effect" : "Allow",
      "Action" : [
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder"
      ],
      "Resource" : [
        "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForNetworkFlowMonitorTopologyService/*"
      ]
    },
    {
      "Sid" : "ConfigRecorderDescribe",
```

```
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ConfigRecorderSlrCreation",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "config.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchNetworkMonitorServiceRolePolicy

Deskripsi: Men CloudWatch gizinkan Monitor Jaringan mengakses dan mengelola sumber daya EC2 dan VPC, mempublikasikan data ke CloudWatch dan mengakses layanan lain yang diperlukan atas nama Anda.

`CloudWatchNetworkMonitorServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 21 Desember 2023, 18:53 UTC
- Waktu teredit: 25 Agustus 2026, 13:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PublishCw",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/NetworkMonitor"
        }
      }
    },
    {
```

```
      "Sid" : "DescribeAny",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteModifyEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ManagedByCloudWatchNetworkMonitor" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchOmniAWSIntegrationPolicy

Deskripsi: Memberikan izin yang diperlukan oleh CloudWatch Omni untuk menemukan dan membaca topologi AWS sumber daya

`CloudWatchOmniAWSIntegrationPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchOmniAWSIntegrationPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 September 2026, 04:07 UTC
- Waktu teredit: 22 September 2026, 04:07 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOmniAWSIntegrationPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "ResourceDiscoveryReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "airflow:GetEnvironment",
        "airflow:List*",
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:List*",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetEnvironment",
        "appconfig:List*",
        "application-autoscaling:Describe*",
        "apprunner:Describe*",
        "apprunner:List*",
        "appsync:GetApiAssociation",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
        "appsync:GetFunction",
        "appsync:GetGraphqlApi",
        "appsync:GetResolver",
        "appsync:GetSourceApiAssociation",
        "appsync:List*",
        "athena:GetDataCatalog",
        "athena:GetWorkGroup",
        "athena:List*",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAccountSettings",
        "autoscaling:DescribeAdjustmentTypes",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeAutoScalingNotificationTypes",
        "autoscaling:DescribeInstanceRefreshes",
        "autoscaling:DescribeLifecycleHookTypes",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribeLoadBalancerTargetGroups",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeMetricCollectionTypes",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribePolicies",
```

```
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScalingProcessTypes",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeTerminationPolicyTypes",
        "autoscaling:DescribeTrafficSources",
        "autoscaling:DescribeWarmPool",
        "batch:Describe*",
        "batch:List*",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetDataSource",
        "bedrock:GetGuardrail",
        "bedrock:GetKnowledgeBase",
        "bedrock:List*",
        "cloudformation:Describe*",
        "cloudformation:GetResource",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:List*",
        "cloudfront:Describe*",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:List*",
        "cloudtrail:Describe*",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:List*",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetLogDeliveryConfiguration",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "config:BatchGetAggregateResourceConfig",
        "config:BatchGetResourceConfig",
        "config:Describe*",
        "config:GetAggregateResourceConfig",
```

```
        "config:GetResourceConfigHistory",
        "config:GetStoredQuery",
        "config:List*",
        "config:SelectAggregateResourceConfig",
        "config:SelectResourceConfig",
        "dax:DescribeClusters",
        "dax:ListTags",
        "directconnect:Describe*",
        "dms:Describe*",
        "dms:List*",
        "dynamodb:Describe*",
        "dynamodb:GetResourcePolicy",
        "dynamodb:List*",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAccountVpcEncryptionControl",
        "ec2:DescribeAddressTransfers",
        "ec2:DescribeAddresses",
        "ec2:DescribeAddressesAttribute",
        "ec2:DescribeAggregateIdFormat",
        "ec2:DescribeApplicationStatus",
        "ec2:DescribeApplicationStatusCheckAssociations",
        "ec2:DescribeApplicationStatusChecks",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAwsNetworkPerformanceMetricSubscriptions",
        "ec2:DescribeBundleTasks",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeCapacityBlockExtensionHistory",
        "ec2:DescribeCapacityBlockExtensionOfferings",
        "ec2:DescribeCapacityBlockOfferings",
        "ec2:DescribeCapacityBlockStatus",
        "ec2:DescribeCapacityBlocks",
        "ec2:DescribeCapacityManagerDataExports",
        "ec2:DescribeCapacityReservationBillingRequests",
        "ec2:DescribeCapacityReservationCancellationQuotes",
        "ec2:DescribeCapacityReservationFleets",
        "ec2:DescribeCapacityReservationTopology",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeClientVpnAuthorizationRules",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeClientVpnRoutes",
        "ec2:DescribeClientVpnTargetNetworks",
        "ec2:DescribeCoipPools",
```

```
        "ec2:DescribeConversionTasks",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDeclarativePoliciesReports",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeElasticGpus",
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeExportTasks",
        "ec2:DescribeFastLaunchImages",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DescribeFleetHistory",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeFpgaImageAttribute",
        "ec2:DescribeFpgaImages",
        "ec2:DescribeHostReservationOfferings",
        "ec2:DescribeHostReservations",
        "ec2:DescribeHosts",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeIdFormat",
        "ec2:DescribeIdentityIdFormat",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeImageReferences",
        "ec2:DescribeImageUsageReportEntries",
        "ec2:DescribeImageUsageReports",
        "ec2:DescribeImages",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeImportSnapshotTasks",
        "ec2:DescribeInstanceConnectEndpoints",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeInstanceEventNotificationAttributes",
        "ec2:DescribeInstanceEventWindows",
        "ec2:DescribeInstanceImageMetadata",
        "ec2:DescribeInstanceSqlHaHistoryStates",
        "ec2:DescribeInstanceSqlHaStates",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTopology",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamByoasn",
        "ec2:DescribeIpamExternalResourceVerificationTokens",
```

```
        "ec2:DescribeIpamInternetRegistryAssociations",
        "ec2:DescribeIpamPolicies",
        "ec2:DescribeIpamPoolAllocations",
        "ec2:DescribeIpamPools",
        "ec2:DescribeIpamPrefixListResolverTargets",
        "ec2:DescribeIpamPrefixListResolvers",
        "ec2:DescribeIpamResourceDiscoveries",
        "ec2:DescribeIpamResourceDiscoveryAssociations",
        "ec2:DescribeIpamScopes",
        "ec2:DescribeIpams",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeLockedSnapshots",
        "ec2:DescribeMacHosts",
        "ec2:DescribeMacModificationTasks",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeOutpostLags",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePrefixLists",
        "ec2:DescribePrincipalIdFormat",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeRegions",
        "ec2:DescribeReplaceRootVolumeTasks",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeReservedInstancesListings",
        "ec2:DescribeReservedInstancesModifications",
        "ec2:DescribeReservedInstancesOfferings",
```

```
        "ec2:DescribeRouteServerEndpoints",
        "ec2:DescribeRouteServerPeers",
        "ec2:DescribeRouteServers",
        "ec2:DescribeRouteTables",
        "ec2:DescribeScheduledInstanceAvailability",
        "ec2:DescribeScheduledInstances",
        "ec2:DescribeSecondaryInterfaces",
        "ec2:DescribeSecondaryNetworks",
        "ec2:DescribeSecondarySubnets",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeServiceLinkVirtualInterfaces",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotDatafeedSubscription",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeStoreImageTasks",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilterRules",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayMeteringPolicies",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:DescribeTransitGatewayRouteTableAnnouncements",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTrunkInterfaceAssociations",
        "ec2:DescribeVerifiedAccessEndpoints",
        "ec2:DescribeVerifiedAccessGroups",
        "ec2:DescribeVerifiedAccessInstanceLoggingConfigurations",
```

```
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessTrustProviders",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcBlockPublicAccessExclusions",
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEncryptionControls",
        "ec2:DescribeVpcEndpointAssociations",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConcentrators",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayRoutes",
        "ecr:Describe*",
        "ecr:GetRepositoryPolicy",
        "ecr:List*",
        "ecs:Describe*",
        "ecs:List*",
        "eks:Describe*",
        "eks:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticfilesystem:Describe*",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:GetResourcePolicy",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
```

```
        "emr-containers:Describe*",
        "emr-containers:List*",
        "emr-serverless:GetApplication",
        "emr-serverless:List*",
        "es:Describe*",
        "es:List*",
        "events:Describe*",
        "events:List*",
        "firehose:Describe*",
        "firehose:List*",
        "fsx:Describe*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetJob",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTrigger",
        "glue:GetWorkflow",
        "glue:List*",
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAccountAliases",
        "iam:ListAttachedRolePolicies",
        "iam:ListOpenIDConnectProviders",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "kafka:Describe*",
        "kafka:GetClusterPolicy",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kinesis:Describe*",
        "kinesis:GetResourcePolicy",
        "kinesis:List*",
        "kinesisanalytics:Describe*",
        "kinesisanalytics:List*",
```

```
        "kinesisvideo:Describe*",
        "kinesisvideo:List*",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:ListAliases",
        "kms:ListGrants",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:List*",
        "memorydb:Describe*",
        "memorydb:List*",
        "mq:Describe*",
        "mq:List*",
        "networkmanager:Describe*",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetVpcAttachment",
        "networkmanager:List*",
        "organizations:Describe*",
        "organizations:List*",
        "osis:GetPipeline",
        "osis:List*",
        "pipes:Describe*",
        "pipes:List*",
        "ram:GetPermission",
```

```
        "ram:GetResourceShares",
        "ram:List*",
        "rds:Describe*",
        "rds:List*",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
        "redshift:Describe*",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:List*",
        "resource-explorer-2:Search",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:List*",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:List*",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:List*",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:List*",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketNotification",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetEncryptionConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
```

```
        "scheduler:List*",
        "secretsmanager:Describe*",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:List*",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:List*",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:List*",
        "ses:GetAccount",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetEmailIdentity",
        "ses:ListConfigurationSets",
        "ses:ListEmailIdentities",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:List*",
        "ssm:Describe*",
        "ssm:ListAssociationVersions",
        "ssm:ListAssociations",
        "ssm:ListCloudConnectors",
        "ssm:ListCommands",
        "ssm:ListComplianceItems",
        "ssm:ListComplianceSummaries",
        "ssm:ListDocumentMetadataHistory",
        "ssm:ListDocumentVersions",
        "ssm:ListDocuments",
        "ssm:ListInventoryEntries",
        "ssm:ListNodes",
        "ssm:ListNodesSummary",
        "ssm:ListOpsItemEvents",
        "ssm:ListOpsItemRelatedItems",
        "ssm:ListOpsMetadata",
        "ssm:ListResourceComplianceSummaries",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeMapRun",
        "states:DescribeStateMachine",
```

```
        "states:DescribeStateMachineAlias",
        "states:DescribeStateMachineForExecution",
        "states:List*",
        "tag:GetResources",
        "timestream:Describe*",
        "timestream:List*",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetAuthPolicy",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integrations",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integrations/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/domainnames",
```

```
        "arn:aws:apigateway:*::/domainnames/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchOmniDomainAccessPolicy

Deskripsi: Menyediakan izin yang diperlukan untuk mengelola akses domain CloudWatch Omni.

`CloudWatchOmniDomainAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchOmniDomainAccessPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 September 2026, 01:47 UTC
- Waktu teredit: 22 September 2026, 01:47 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOmniDomainAccessPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchOmniDomainAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListSpacesForOrganization",
        "cloudwatch:CreateDomainAccessGrantForOrganization",
        "cloudwatch:GetDomainAccessGrantForOrganization",
        "cloudwatch:ListDomainAccessGrantsForOrganization",
        "cloudwatch:DeleteDomainAccessGrantForOrganization"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "cloudwatch:HasAccessGrant" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchOmniModelInferencePolicy

Deskripsi: Kebijakan terkelola bagi pelanggan untuk dilampirkan ke CloudWatch Omni sehingga fitur CloudWatch Omni dapat melakukan panggilan Inferensi Model Bedrock seperti di Taman Bermain Agen atau Evaluasi

`CloudWatchOmniModelInferencePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchOmniModelInferencePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 September 2026, 01:47 UTC
- Waktu teredit: 22 September 2026, 01:47 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOmniModelInferencePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AgentCoreEvaluationBedrockInvoke",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "AgentCoreEvaluationBedrockMantleInference",
      "Effect" : "Allow",
      "Action" : "bedrock-mantle:CreateInference",
      "Resource" : "arn:aws:bedrock-mantle:*:*:project/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AgentCoreEvaluationBedrockMantleCallWithBearerToken",
      "Effect" : "Allow",
      "Action" : "bedrock-mantle:CallWithBearerToken",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchOmniSpaceAccessPolicy

Deskripsi: Menyediakan akses untuk mengelola ruang CloudWatch Omni, melihat Telemetri Aplikasi, dan fitur Observabilitas dan Pemantauan lainnya melalui Produk Omni baru CloudWatch

`CloudWatchOmniSpaceAccessPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchOmniSpaceAccessPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 September 2026, 01:47 UTC
- Waktu teredit: 22 September 2026, 01:47 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOmniSpaceAccessPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchOmniSpaceAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:UpdateSpace",
        "cloudwatch:GetSpace",
        "cloudwatch:ListSpaces",
        "cloudwatch:GetDomain",
        "cloudwatch:CreateAccessGrant",
        "cloudwatch:GetAccessGrant",
        "cloudwatch:ListAccessGrants",
        "cloudwatch:DeleteAccessGrant",
        "cloudwatch:SearchPrincipals",
        "cloudwatch:StartTelemetryQuerySession",
        "cloudwatch:StopTelemetryQuerySession",
        "cloudwatch:ListTelemetryQuerySessions",
        "cloudwatch:StopTelemetryQuery",
        "cloudwatch:GetTelemetryQueryResults",
        "cloudwatch:GetRecords",
        "cloudwatch:GetMetricData",
```

```
        "cloudwatch:ListMetrics",
        "cloudwatch:GetContextGraph",
        "cloudwatch:CreateAlert",
        "cloudwatch:GetAlert",
        "cloudwatch:UpdateAlert",
        "cloudwatch:DeleteAlert",
        "cloudwatch:ListAlerts",
        "cloudwatch:CreateOmniDashboard",
        "cloudwatch:GetOmniDashboard",
        "cloudwatch:UpdateOmniDashboard",
        "cloudwatch:DeleteOmniDashboard",
        "cloudwatch:ListOmniDashboards",
        "cloudwatch:CreateAccessProfile",
        "cloudwatch:GetAccessProfile",
        "cloudwatch:UpdateAccessProfile",
        "cloudwatch:DeleteAccessProfile",
        "cloudwatch:ListAccessProfiles",
        "cloudwatch:AssumeAccessProfile",
        "cloudwatch:CreateView",
        "cloudwatch:GetView",
        "cloudwatch:UpdateView",
        "cloudwatch:DeleteView",
        "cloudwatch:ListViews",
        "cloudwatch:GetPreferences",
        "cloudwatch:UpdatePreferences",
        "cloudwatch:CreateOmniThread",
        "cloudwatch:GetOmniThread",
        "cloudwatch:UpdateOmniThread",
        "cloudwatch:ListOmniThreads",
        "cloudwatch:DeleteOmniThread",
        "cloudwatch:StartOmniThreadSession",
        "cloudwatch:SubmitFeedback",
        "cloudwatch:CreateIntegration",
        "cloudwatch:UpdateIntegration",
        "cloudwatch:GetIntegration",
        "cloudwatch:DeleteIntegration",
        "cloudwatch:ListIntegrations",
        "cloudwatch:InvokeIntegration",
        "cloudwatch:GetIntelligenceConfiguration",
        "cloudwatch:PutIntelligenceConfiguration",
        "cloudwatch:TagResource",
        "cloudwatch:UntagResource",
        "cloudwatch:ListTagsForResource"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:HasAccessGrant" : "true"
        }
      }
    },
    {
      "Sid" : "DenyClassicCloudWatchResourceTagging",
      "Effect" : "Deny",
      "Action" : [
        "cloudwatch:TagResource",
        "cloudwatch:UntagResource",
        "cloudwatch:ListTagsForResource"
      ],
      "NotResource" : [
        "arn:aws:cloudwatch:*:*:space/*",
        "arn:aws:cloudwatch:*:*:domain/*",
        "arn:aws:cloudwatch:*:*:organization-domain/*",
        "arn:aws:cloudwatch:*:*:access-grant/*",
        "arn:aws:cloudwatch:*:*:organization-access-grant/*",
        "arn:aws:cloudwatch:*:*:access-profile/*",
        "arn:aws:cloudwatch:*:*:omni-dashboard/*",
        "arn:aws:cloudwatch:*:*:alert/*",
        "arn:aws:cloudwatch:*:*:view/*",
        "arn:aws:cloudwatch:*:*:integration/*",
        "arn:aws:cloudwatch:*:*:dataset/*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForCloudWatchOmni",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "cloudwatch.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "ListRolesAndUsers",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers",
        "iam:ListRoles",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIKeyConfigurationUsers",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUserTags",
        "iam:ListServiceSpecificCredentials"
      ],
      "Resource" : "arn:aws:iam::*:user/omni/OmniIngestionUser-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KmsListKeysForOmni",
      "Effect" : "Allow",
      "Action" : "kms:ListKeys",
      "Resource" : "*"
    },
    {
      "Sid" : "KmsDescribeKeyForOmni",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "KmsCryptoOpsForOmniSpaces",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudwatch.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/cw-omni" : "true"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:cloudwatch:arn" : "arn:aws:cloudwatch:*:
${aws:PrincipalAccount}:space/*"
        }
      }
    },
    {
      "Sid" : "KmsCryptoOpsForDatasets",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudwatch.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:cloudwatch:arn" : "arn:aws:cloudwatch:*:
${aws:PrincipalAccount}:dataset/*"
        }
```

```
      }
    },
    {
      "Sid" : "KmsCryptoOpsForOmniIntelligence",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudwatch.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/cw-omni" : "true"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:cloudwatch:account" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KmsCryptoOpsForOmniIntelligenceBranchKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudwatch.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/cw-omni" : "true"
        },
        "StringLike" : {
```

```
          "kms:EncryptionContext:aws-crypto-ec:aws:cloudwatch:account" :
 "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ConfigServiceLinkedRecorderManagement",
      "Effect" : "Allow",
      "Action" : [
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "config:ConfigurationRecorderServicePrincipal" : [
            "cloudwatch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeConfigurationRecorder",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowConfigServiceLinkedRoleCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:AWSServiceName" : "config.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "AgentCoreEvaluator",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:CreateEvaluator",
        "bedrock-agentcore:GetEvaluator",
        "bedrock-agentcore:UpdateEvaluator",
        "bedrock-agentcore:DeleteEvaluator",
        "bedrock-agentcore:ListEvaluators",
        "bedrock-agentcore:Evaluate",
        "bedrock-agentcore:TagResource",
        "bedrock-agentcore:UntagResource",
        "bedrock-agentcore:ListTagsForResource"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:evaluator/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AgentCoreOnlineEvaluationConfig",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:CreateOnlineEvaluationConfig",
        "bedrock-agentcore:GetOnlineEvaluationConfig",
        "bedrock-agentcore:ListOnlineEvaluationConfigs",
        "bedrock-agentcore:UpdateOnlineEvaluationConfig",
        "bedrock-agentcore:DeleteOnlineEvaluationConfig",
        "bedrock-agentcore:TagResource",
        "bedrock-agentcore:UntagResource",
        "bedrock-agentcore:ListTagsForResource"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:online-evaluation-config/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "AgentCoreEvaluationDatasets",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GetDataset",
        "bedrock-agentcore:ListDatasets",
        "bedrock-agentcore:ListDatasetVersions",
        "bedrock-agentcore:ListDatasetExamples",
        "bedrock-agentcore:CreateDataset",
        "bedrock-agentcore:UpdateDataset",
        "bedrock-agentcore:CreateDatasetVersion",
        "bedrock-agentcore:AddDatasetExamples",
        "bedrock-agentcore:UpdateDatasetExamples",
        "bedrock-agentcore:DeleteDatasetExamples",
        "bedrock-agentcore:DeleteDataset",
        "bedrock-agentcore:TagResource",
        "bedrock-agentcore:UntagResource",
        "bedrock-agentcore:ListTagsForResource"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:dataset/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockFoundationModelDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AgentCorePassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "bedrock-agentcore.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AnnotationAndEvalLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/cloudwatch/*",
        "arn:aws:logs:*:*:log-group:/aws/bedrock-agentcore/evaluations/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "OnlineEvalLogGroupDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KmsCryptoOpsForCMKEvaluators",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
```

```
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:bedrock-agentcore:evaluatorArn" :
"arn:aws:bedrock-agentcore:*:${aws:PrincipalAccount}:evaluator/*"
        }
      }
    },
    {
      "Sid" : "CodeEvaluatorLambdaInvoke",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:GetFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:cloudwatchCodeEvaluator*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ModelProviderKeyDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModelProviderKeyCreation",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:cw-omni-*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/cw-omni" : "true",
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ModelProviderKeyManagement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutSecretValue",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:cw-omni-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/cw-omni" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchOpenSearchDashboardAccess

Deskripsi: Kebijakan ini menyediakan akses pengguna untuk melihat OpenSearch dasbor di konsol CloudWatch Log.

`CloudWatchOpenSearchDashboardAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchOpenSearchDashboardAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2024, 21:06 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOpenSearchDashboardAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchOpenSearchDashboardsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "logs:ListIntegrations",
        "logs:GetIntegration",
        "logs:DescribeLogGroups",
        "opensearch:ApplicationAccessAll",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsOpensearchReadAPIs",
```

```
      "Effect" : "Allow",
      "Action" : [
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "es:ListApplications"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsAPIAccessAll",
      "Effect" : "Allow",
      "Action" : [
        "aoss:APIAccessAll"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "cloudwatch-logs-*"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsDQSCollectionPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aoss:collection" : "cloudwatch-logs-*"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsApplicationResourceAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "es:GetApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/OpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsDQSResourceQueryAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:GetDirectQueryDataSource"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsDirectQueryStatusAccess",
      "Effect" : "Allow",
      "Action" : [
        "opensearch:GetDirectQuery"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchOpenSearchDashboardsFullAccess

Deskripsi: Kebijakan ini menyediakan akses pengguna untuk membuat integrasi OpenSearch untuk membuat, memperbarui, menghapus, atau melihat dasbor di konsol CloudWatch Log.

`CloudWatchOpenSearchDashboardsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchOpenSearchDashboardsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2024, 21:06 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOpenSearchDashboardsFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchOpenSearchDashboardsIntegration",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:ListIntegrations",
        "logs:GetIntegration",
        "logs:DeleteIntegration",
        "logs:PutIntegration",
        "logs:DescribeLogGroups",
        "opensearch:ApplicationAccessAll",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsOpensearchReadAPIs",
      "Effect" : "Allow",
      "Action" : [
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "es:ListApplications"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsOpensearchCreateServiceLinkedAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
opensearchservice.amazonaws.com/AWSServiceRoleForAmazonOpenSearchService",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "opensearchservice.amazonaws.com",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "CloudWatchLogsObservabilityCreateServiceLinkedAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
observability.aoss.amazonaws.com/AWSServiceRoleForAmazonOpenSearchServerless",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "observability.aoss.amazonaws.com",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsCollectionRequestAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:CreateCollection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:RequestTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsApplicationRequestAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:CreateApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:RequestTag/OpenSearchIntegration" : [
```

```
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "OpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsCollectionResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:DeleteCollection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsApplicationResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:UpdateApplication",
        "es:GetApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/OpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsCollectionPolicyAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "aoss:CreateSecurityPolicy",
        "aoss:CreateAccessPolicy",
        "aoss:DeleteAccessPolicy",
        "aoss:DeleteSecurityPolicy",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "cloudwatch-logs-*",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsAPIAccessAll",
      "Effect" : "Allow",
      "Action" : [
        "aoss:APIAccessAll"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "cloudwatch-logs-*"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsIndexPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:CreateAccessPolicy",
        "aoss:DeleteAccessPolicy",
        "aoss:GetAccessPolicy",
        "aoss:CreateLifecyclePolicy",
        "aoss:DeleteLifecyclePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:index" : "cloudwatch-logs-*",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsDQSRequestQueryAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:AddDirectQueryDataSource"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:RequestTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsStartDirectQueryAccess",
      "Effect" : "Allow",
      "Action" : [
        "opensearch:StartDirectQuery",
        "opensearch:GetDirectQuery"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*"
    },
    {
      "Sid" : "CloudWatchLogsDQSResourceQueryAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:GetDirectQueryDataSource",
        "es:DeleteDirectQueryDataSource"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "directquery.opensearchservice.amazonaws.com",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsAossTagsAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:TagResource"
      ],
      "Resource" : "arn:aws:aoss:*:*:collection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsEsApplicationTagsAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:AddTags"
      ],
      "Resource" : "arn:aws:opensearch:*:*:application/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OpenSearchIntegration" : [
            "Dashboards"
          ],
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "OpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsEsDataSourceTagsAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:AddTags"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ],
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke CloudWatch.

`CloudWatchReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 22 September 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v25 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:BatchGet*",
        "application-signals:Get*",
        "application-signals:List*",
        "autoscaling:Describe*",
        "cloudtrail:ListChannels",
```

```
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudwatch:CreateOneTimeDeepLinkCode",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "oam:ListSinks",
        "observabilityadmin:GetCentralizationRuleForOrganization",
        "observabilityadmin:ListCentralizationRulesForOrganization",
        "observabilityadmin:GetTelemetryEvaluationStatus",
        "observabilityadmin:GetTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:GetTelemetryRule",
        "observabilityadmin:GetTelemetryRuleForOrganization",
        "observabilityadmin:ListResourceTelemetry",
        "observabilityadmin:ListResourceTelemetryForOrganization",
        "observabilityadmin:ListTelemetryRules",
        "observabilityadmin:ListTelemetryRulesForOrganization",
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:ListTagsForResource",
        "observabilityadmin:GetTelemetryPipeline",
        "observabilityadmin:ListTelemetryPipelines",
        "observabilityadmin:TestTelemetryPipeline",
        "observabilityadmin:ValidateTelemetryPipelineConfiguration",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:GetDatasetIntegration",
        "observabilityadmin:ListDatasetIntegrations",
        "sns:Get*",
        "sns:List*",
        "rum:BatchGet*",
        "rum:Get*",
        "rum:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
```

```
        "xray:BatchGet*",
        "xray:Get*",
        "xray:List*",
        "xray:StartTraceRetrieval",
        "xray:CancelTraceRetrieval"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchReadOnlyGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
```

```
        "arn:aws:servicequotas:*:*:lambda/*",
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
    },
    {
      "Sid" : "CloudWatchResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchSyntheticsFullAccess

Deskripsi: Menyediakan akses penuh ke S CloudWatch intetis.

`CloudWatchSyntheticsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchSyntheticsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 November 2019, 17:39 UTC
- Waktu teredit: 31 Maret 2026, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess`

Versi kebijakan

Versi kebijakan: v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::cw-syn-results-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*/exports/swagger",
        "arn:aws:apigateway:*::/apis"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::cw-syn-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::aws-synthetics-library-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "synthetics.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:Synthetics-*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogRecord",
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:GetLogGroupFields"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/cwsyn-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:AddPermission",
        "lambda:PublishVersion",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunction",
        "lambda:DeleteFunction",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:cwsyn-*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetLayerVersion",
        "lambda:PublishLayerVersion",
        "lambda:DeleteLayerVersion"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:layer:cwsyn-*",
        "arn:aws:lambda:*:*:layer:Synthetics:*",
        "arn:aws:lambda:*:*:layer:Synthetics_Selenium:*",
        "arn:aws:lambda:*:*:layer:AWS-CW-Synthetics*:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : [
```

```
        "arn:*:sns:*:*:Synthetics-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CloudWatchSyntheticsReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke CloudWatch Synthetics.

`CloudWatchSyntheticsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchSyntheticsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 November 2019, 17:45 UTC
- Waktu teredit: 06 Maret 2020, 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ComprehendDataAccessRolePolicy

Deskripsi: Kebijakan untuk AWS peran layanan Memahami yang memungkinkan akses ke sumber daya S3 untuk akses data

`ComprehendDataAccessRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ComprehendDataAccessRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Maret 2019, 22:28 UTC
- Waktu teredit: 06 Maret 2019, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::*Comprehend*",
      "arn:aws:s3:::*comprehend*"
    ]
  }
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ComprehendFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Comprecept.

`ComprehendFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ComprehendFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 29 November 2017, 18:08 UTC
- Waktu teredit: 05 Desember 2017, 01:36 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehend:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ComprehendMedicalFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Compredeh Medical

`ComprehendMedicalFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ComprehendMedicalFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2018, 17:55 UTC
- Waktu teredit: 27 November 2018, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendMedicalFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehendmedical:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ComprehendReadOnly

Deskripsi: Menyediakan akses baca-saja ke Amazon Comprecept.

`ComprehendReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ComprehendReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2017, 18:10 UTC
- Waktu teredit: 26 April 2022, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendReadOnly`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
    "Effect" : "Allow",
    "Action" : [
      "comprehend:DetectDominantLanguage",
      "comprehend:BatchDetectDominantLanguage",
      "comprehend:DetectEntities",
      "comprehend:BatchDetectEntities",
      "comprehend:DetectKeyPhrases",
      "comprehend:BatchDetectKeyPhrases",
      "comprehend:DetectPiiEntities",
      "comprehend:ContainsPiiEntities",
      "comprehend:DetectSentiment",
      "comprehend:BatchDetectSentiment",
      "comprehend:DetectSyntax",
      "comprehend:BatchDetectSyntax",
      "comprehend:ClassifyDocument",
      "comprehend:DescribeTopicsDetectionJob",
      "comprehend:ListTopicsDetectionJobs",
      "comprehend:DescribeDominantLanguageDetectionJob",
      "comprehend:ListDominantLanguageDetectionJobs",
      "comprehend:DescribeEntitiesDetectionJob",
      "comprehend:ListEntitiesDetectionJobs",
      "comprehend:DescribeKeyPhrasesDetectionJob",
      "comprehend:ListKeyPhrasesDetectionJobs",
      "comprehend:DescribePiiEntitiesDetectionJob",
      "comprehend:ListPiiEntitiesDetectionJobs",
      "comprehend:DescribeSentimentDetectionJob",
      "comprehend:DescribeTargetedSentimentDetectionJob",
      "comprehend:ListSentimentDetectionJobs",
      "comprehend:ListTargetedSentimentDetectionJobs",
      "comprehend:DescribeDocumentClassifier",
      "comprehend:ListDocumentClassifiers",
      "comprehend:DescribeDocumentClassificationJob",
      "comprehend:ListDocumentClassificationJobs",
      "comprehend:DescribeEntityRecognizer",
      "comprehend:ListEntityRecognizers",
      "comprehend:ListTagsForResource",
      "comprehend:DescribeEndpoint",
      "comprehend:ListEndpoints",
      "comprehend:ListDocumentClassifierSummaries",
      "comprehend:ListEntityRecognizerSummaries",
      "comprehend:DescribeResourcePolicy"
    ],
    "Resource" : "*"
  }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ComputeOptimizerAutomationServiceRolePolicy

Deskripsi: Kebijakan ComputeOptimizerAutomationServiceRolePolicy terkelola dilampirkan ke peran terkait layanan yang memungkinkan Compute Optimizer melakukan tindakan atas nama Anda

`ComputeOptimizerAutomationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 15 November 2025, 01:19 UTC
- Waktu teredit: 15 November 2025, 01:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerAutomationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumesModifications"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EBSVolumeModification",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/exclude-from-compute-optimizer-automation" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEBSSnapshot",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RollbackEBSVolumeDeletion",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Tag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ComputeOptimizerReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke ComputeOptimizer.

`ComputeOptimizerReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ComputeOptimizerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Maret 2020, 00:11 UTC
- Waktu teredit: 20 November 2024, 21:08 UTC
- ARN: `arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "computeOptimizerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:DescribeRecommendationExportJobs",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:GetEnrollmentStatusesForOrganization",
        "compute-optimizer:GetRecommendationSummaries",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEC2RecommendationProjectedMetrics",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEBSVolumeRecommendations",
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetRecommendationPreferences",
```

```
        "compute-optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetECSServiceRecommendations",
        "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:GetRDSDatabaseRecommendations",
        "compute-optimizer:GetRDSDatabaseRecommendationProjectedMetrics",
        "compute-optimizer:GetLicenseRecommendations",
        "compute-optimizer:GetIdleRecommendations",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ecs:ListServices",
        "ecs:ListClusters",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "lambda:ListFunctions",
        "lambda:ListProvisionedConcurrencyConfigs",
        "cloudwatch:GetMetricData",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ComputeOptimizerServiceRolePolicy

Deskripsi: Memungkinkan ComputeOptimizer untuk menelepon AWS layanan dan mengumpulkan detail beban kerja atas nama Anda.

`ComputeOptimizerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 03 Desember 2019, 08:45 UTC
- Waktu teredit: 27 Mei 2026, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ComputeOptimizerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
```

```
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudWatchAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingAccess",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2Access",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ElastiCacheAccess",
      "Effect" : "Allow",
      "Action" : [
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeServerlessCaches"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MemoryDBAccess",
      "Effect" : "Allow",
      "Action" : [
        "memorydb:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DocumentDBAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBAccess",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "WorkSpacesAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspacesConnectionStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListEndpoints",
        "sagemaker:DescribeEndpoint"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ConfigConformsServiceRolePolicy

Deskripsi: Kebijakan yang diperlukan untuk AWSConfig untuk membuat paket kesesuaian

`ConfigConformsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 25 Juli 2019, 21:38 UTC
- Waktu teredit: 12 Januari 2023, 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule",
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/config-
conforms.amazonaws.com*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigRules"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeRemediationConfigurations",
        "config:DeleteRemediationConfiguration",
        "config:PutRemediationConfigurations"
      ],
      "Resource" : "arn:aws:config:*:*:remediation-configuration/aws-service-
remediation-configuration/config-conforms.amazonaws.com*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
remediation.config.amazonaws.com/AWSServiceRoleForConfigRemediation"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
remediation.config.amazonaws.com/AWSServiceRoleForConfigRemediation",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "remediation.config.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:GetObject",
        "s3:GetBucketAcl"
      ],
      "Resource" : "arn:aws:s3:::awsconfigconforms*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:GetStackPolicy",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:ValidateTemplate",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/awsconfigconforms-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Config"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ConsoleFullAccessFromVercel

Deskripsi: Untuk digunakan dengan akun yang dibuat melalui integrasi Vercel Marketplace dengan AWS. Menyediakan akses untuk mengelola semua sumber daya untuk layanan yang terintegrasi dengan Vercel Marketplace.

`ConsoleFullAccessFromVercel`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ConsoleFullAccessFromVercel` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Desember 2025, 16:49 UTC
- Waktu teredit: 09 April 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/ConsoleFullAccessFromVercel`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSQL",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
        "dsql:UpdateCluster",
```

```
        "dsql:DbConnectAdmin",
        "dsql:DbConnect"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DynamoDB",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchGetItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:UpdateTimeToLive",
        "dynamodb:ConditionCheckItem",
        "dynamodb:UntagResource",
        "dynamodb:PutItem",
        "dynamodb:ListTables",
        "dynamodb:DeleteItem",
        "dynamodb:Scan",
        "dynamodb:ListTagsOfResource",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:TagResource",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:DescribeLimits",
        "dynamodb:UpdateTable",
        "dynamodb:GetRecords"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Aurora",
      "Effect" : "Allow",
      "Action" : [
        "rds-db:connect",
        "rds:Describe*",
        "rds:ListTagsForResource",
        "rds:RebootDBInstance",
        "rds:DeleteDBInstance",
```

```
        "rds:StartDBInstance",
        "rds:ModifyDBInstance",
        "rds:ApplyPendingMaintenanceAction",
        "rds:StartDBCluster",
        "rds:DeleteDBCluster",
        "rds:RebootDBCluster",
        "rds:CreateDBClusterEndpoint",
        "rds:ModifyDBClusterEndpoint",
        "rds:ModifyDBCluster",
        "rds:DeleteDBClusterEndpoint",
        "rds:FailoverDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:ModifyDBClusterParameterGroup",
        "rds:CopyDBClusterParameterGroup",
        "rds:ResetDBClusterParameterGroup",
        "rds:CreateDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:ModifyDBParameterGroup",
        "rds:CopyDBParameterGroup",
        "rds:DeleteDBParameterGroup",
        "rds:CreateDBParameterGroup",
        "rds:DeleteDBClusterAutomatedBackup",
        "rds:CopyDBClusterSnapshot",
        "rds:RestoreDBClusterToPointInTime",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:CreateDBClusterSnapshot",
        "rds:DeleteDBClusterSnapshot",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AuroraRestricted",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "rds:DatabaseEngine" : "aurora-postgresql"
        }
      }
    },
    {
      "Sid" : "OpenSearchServerless",
      "Effect" : "Allow",
      "Action" : [
        "aoss:APIAccessAll",
        "aoss:DashboardsAccessAll",
        "aoss:BatchGetCollection",
        "aoss:BatchGetCollectionGroup",
        "aoss:CreateIndex",
        "aoss:DeleteIndex",
        "aoss:GetAccessPolicy",
        "aoss:GetIndex",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollectionGroups",
        "aoss:ListCollections",
        "aoss:ListSecurityPolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListTagsForResource",
        "aoss:TagResource",
        "aoss:UntagResource",
        "aoss:AddCollectionToCollectionGroup",
        "aoss:UpdateAccessPolicy",
        "aoss:UpdateCollection",
        "aoss:UpdateCollectionGroup",
        "aoss:UpdateIndex",
        "aoss:UpdateSecurityPolicy"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OpenSearchApplications",
      "Effect" : "Allow",
      "Action" : [
        "es:GetApplication",
        "es:UpdateApplication",
        "es:ListApplications",
        "es:GetDefaultApplicationSetting"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Observability",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ApplicationAutoscalingIntegration",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "dynamodb"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingDescribeActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ViewFreeTierState",
      "Effect" : "Allow",
      "Action" : [
        "freetier:GetAccountPlanState"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ConsoleViewOnlyAccessFromVercel

Deskripsi: Untuk digunakan dengan akun yang dibuat melalui integrasi Vercel Marketplace dengan AWS. Menyediakan akses untuk melihat semua sumber daya untuk layanan yang terintegrasi dengan Vercel Marketplace.

`ConsoleViewOnlyAccessFromVercel`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ConsoleViewOnlyAccessFromVercel` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 11 Desember 2025, 16:49 UTC
- Waktu teredit: 09 April 2026, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/ConsoleViewOnlyAccessFromVercel`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSQL",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DynamoDB",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeLimits"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "Aurora",
      "Effect" : "Allow",
      "Action" : [
        "rds:Describe*",
        "rds:ListTagsForResource",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OpenSearchServerless",
      "Effect" : "Allow",
      "Action" : [
        "aoss:BatchGetCollection",
        "aoss:BatchGetCollectionGroup",
        "aoss:GetAccessPolicy",
        "aoss:GetIndex",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollectionGroups",
        "aoss:ListCollections",
        "aoss:ListSecurityPolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OpenSearchApplications",
      "Effect" : "Allow",
      "Action" : [
        "es:GetApplication",
        "es:ListApplications"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "Observability",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ApplicationAutoscalingDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ViewFreeTierState",
      "Effect" : "Allow",
      "Action" : [
        "freetier:GetAccountPlanState"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CostOptimizationHubAdminAccess

Deskripsi: Kebijakan terkelola ini menyediakan akses admin ke Hub Pengoptimalan Biaya.

`CostOptimizationHubAdminAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CostOptimizationHubAdminAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Desember 2023, 00:03 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationHubAdminAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
```

```
        "cost-optimization-hub:UpdateEnrollmentStatus",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:UpdatePreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
        "cost-optimization-hub:ListEfficiencyMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoleForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/cost-optimization-hub.bcm.amazonaws.com/
AWSServiceRoleForCostOptimizationHub"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cost-optimization-hub.bcm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceAccessForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "cost-optimization-hub.bcm.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CostOptimizationHubReadOnlyAccess

Deskripsi: Kebijakan terkelola ini menyediakan akses baca-saja ke Hub Pengoptimalan Biaya.

`CostOptimizationHubReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `CostOptimizationHubReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 Desember 2023, 18:04 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "CostOptimizationHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
        "cost-optimization-hub:ListEfficiencyMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CostOptimizationHubServiceRolePolicy

Deskripsi: Mengizinkan Hub Pengoptimalan Biaya untuk mengambil informasi organisasi dan mengumpulkan data dan metadata terkait pengoptimalan.

`CostOptimizationHubServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran

- Waktu pembuatan: 26 November 2023, 08:03 UTC
- Waktu teredit: 17 Juli 2025, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AwsOrgsScopedAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
```

```
          "organizations:ServicePrincipal" : [
            "cost-optimization-hub.bcm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CostExplorerAccess",
      "Effect" : "Allow",
      "Action" : [
        "ce:ListCostAllocationTags",
        "ce:GetCostAndUsage",
        "ce:GetDimensionValues"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

CustomerProfilesServiceLinkedRolePolicy

Deskripsi: Mengizinkan Profil Pelanggan Amazon Connect mengakses AWS layanan dan sumber daya atas nama Anda.

`CustomerProfilesServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran

- Waktu pembuatan: 07 Maret 2023, 22:56 UTC
- Waktu teredit: 05 Maret 2026, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CustomerProfilesServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/CustomerProfiles"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/profile.amazonaws.com/
AWSServiceRoleForProfile_*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "connect-campaigns:PutProfileOutboundRequestBatch"
      ],
      "Resource" : [
        "arn:aws:connect-campaigns:*:*:campaign/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "profile:BatchGetProfile",
        "profile:GetRecommender",
        "profile:GetCalculatedAttributeForProfile",
        "profile:GetProfileRecommendations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

DatabaseAdministrator

Deskripsi: Memberikan izin akses penuh ke AWS layanan dan tindakan yang diperlukan untuk mengatur dan mengonfigurasi layanan AWS database.

`DatabaseAdministrator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `DatabaseAdministrator` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan fungsi pekerjaan
- Waktu pembuatan: 10 November 2016, 17:25 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC

- ARN: `arn:aws:iam::aws:policy/job-function/DatabaseAdministrator`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:Describe*",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudwatch:PutMetricAlarm",
        "datapipeline:ActivatePipeline",
        "datapipeline:CreatePipeline",
        "datapipeline:DeletePipeline",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:PutPipelineDefinition",
        "datapipeline:QueryObjects",
        "dynamodb:*",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
```

```
        "elasticache:*",
        "iam:ListRoles",
        "iam:GetRole",
        "kms:ListKeys",
        "lambda:CreateEventSourceMapping",
        "lambda:CreateFunction",
        "lambda:DeleteEventSourceMapping",
        "lambda:DeleteFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:Create*",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "pi:CreatePerformanceAnalysisReport",
        "pi:DeletePerformanceAnalysisReport",
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetPerformanceAnalysisReport",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics",
        "pi:ListPerformanceAnalysisReports",
        "pi:ListTagsForResource",
        "pi:TagResource",
        "pi:UntagResource",
        "rds:*",
        "redshift:*",
        "s3:CreateBucket",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Get*",
        "sns:List*",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject*",
        "s3:Get*",
        "s3:List*",
        "s3:PutAccelerateConfiguration",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutBucketWebsite",
        "s3:PutLifecycleConfiguration",
        "s3:PutReplicationConfiguration",
        "s3:PutObject*",
        "s3:Replicate*",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/rds-monitoring-role",
        "arn:aws:iam::*:role/rdbms-lambda-access",
        "arn:aws:iam::*:role/lambda_exec_role",
        "arn:aws:iam::*:role/lambda-dynamodb-*",
        "arn:aws:iam::*:role/lambda-vpc-execution-role",
        "arn:aws:iam::*:role/DataPipelineDefaultRole",
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

DataScientist

Deskripsi: Memberikan izin ke layanan analisis AWS data.

`DataScientist`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `DataScientist` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan fungsi pekerjaan
- Waktu pembuatan: 10 November 2016, 17:28 UTC
- Waktu teredit: 02 September 2026, 23:37 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DataScientist`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "autoscaling:*",
        "cloudwatch:*",
        "cloudformation:DescribeStackEvents",
        "datapipeline:Describe*",
```

```
        "datapipeline:ListPipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:QueryObjects",
        "dynamodb:*",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CancelSpotFleetRequests",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySpotFleetRequest",
        "ec2:RequestSpotInstances",
        "ec2:RequestSpotFleet",
        "elasticfilesystem:*",
        "elasticmapreduce:*",
        "es:*",
        "firehose:*",
        "fsx:DescribeFileSystems",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListRoles",
        "kinesis:*",
        "kms:List*",
        "lambda:Create*",
        "lambda:Delete*",
        "lambda:Get*",
        "lambda:InvokeFunction",
        "lambda:PublishVersion",
        "lambda:Update*",
        "lambda:List*",
        "machinelearning:*",
        "sdb:*",
        "rds:*",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "redshift:*",
        "s3:CreateBucket",
        "sns:CreateTopic",
        "sns:Get*",
```

```
        "sns:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationCreateStackSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Abort*",
        "s3:DeleteObject",
        "s3:Get*",
        "s3:List*",
        "s3:PutAccelerateConfiguration",
        "s3:PutBucketCors",
        "s3:PutBucketLogging",
```

```
        "s3:PutBucketNotification",
        "s3:PutBucketTagging",
        "s3:PutObject",
        "s3:Replicate*",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DataPipelineDefaultRole",
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
        "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
        "arn:aws:iam::*:role/EMR_DefaultRole",
        "arn:aws:iam::*:role/kinesis-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeDomain",
        "sagemaker:ListDomains",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListUserProfiles",
        "sagemaker:*App",
        "sagemaker:ListApps"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

DAXServiceRolePolicy

Deskripsi: Kebijakan ini memungkinkan DAX untuk membuat dan mengelola antarmuka Jaringan, Grup keamanan, Subnet, dan Vpc atas nama pelanggan

`DAXServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 05 Maret 2018, 17:51 UTC
- Waktu teredit: 05 Maret 2018, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

DBModDiscoveryAndAssessment

Deskripsi: Izin Penemuan dan Penilaian untuk konektor database yang digunakan dalam modernisasi database

`DBModDiscoveryAndAssessment`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `DBModDiscoveryAndAssessment` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Maret 2026, 20:27 UTC
- Waktu teredit: 25 Maret 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/DBModDiscoveryAndAssessment`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeInternetGateways",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBSubnetGroups",
        "dms:DescribeEndpoints",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationTasks",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeOrderableReplicationInstances",
        "dms:ListDataProviders",
        "dms:ListInstanceProfiles",
```

```
        "dms:ListMigrationProjects",
        "dms:ModifyReplicationSubnetGroup",
        "secretsmanager:ListSecrets",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "rds:ModifyDBSubnetGroup",
      "Resource" : "arn:aws:rds:*:*:subgrp:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:EnableHttpEndpoint",
        "rds:DisableHttpEndpoint",
        "rds-data:ExecuteStatement"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dms:DescribeTableStatistics",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTaskIndividualAssessments",
        "dms:DescribeApplicableIndividualAssessments"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:task:*",
```

```
        "arn:aws:dms:*:*:assessment-run:*",
        "arn:aws:dms:*:*:instance-profile:*",
        "arn:aws:dms:*:*:data-provider:*",
        "arn:aws:dms:*:*:migration-project:*",
        "arn:aws:dms:*:*:rep:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dms:ListMetadataModelAssessments",
        "dms:ListMetadataModelConversions",
        "dms:ListMetadataModelExports",
        "dms:DescribeMetadataModelImports",
        "dms:DescribeConversionConfiguration",
        "dms:DescribeMetadataModelCreations",
        "dms:DescribeMetadataModel",
        "dms:DescribeMetadataModelChildren",
        "dms:GetTargetSelectionRules"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/dms-vpc-role",
```

```
        "arn:aws:iam::*:role/dms-cloudwatch-logs-role",
        "arn:aws:iam::*:role/dms-secrets-manager-role",
        "arn:aws:iam::*:role/dms-s3-access-role",
        "arn:aws:iam::*:role/aws-service-role/dms.amazonaws.com/
AWSServiceRoleForDMSServerless"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole",
        "arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:SecretArn" : "arn:aws:secretsmanager:*:
${aws:PrincipalAccount}:secret:*",
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

DBModProvisioningAndMigration

Deskripsi: Penyediaan sumber daya dan izin migrasi data untuk konektor database yang digunakan dalam modernisasi database

`DBModProvisioningAndMigration`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `DBModProvisioningAndMigration` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Maret 2026, 20:42 UTC
- Waktu teredit: 25 Maret 2026, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/DBModProvisioningAndMigration`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:UpdateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:atx-db-modernization-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:atx-db-modernization-*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Project" : "atx-db-modernization",
          "aws:RequestTag/Owner" : "database-connector",
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetBucketVersioning"
      ],
      "Resource" : [
        "arn:aws:s3:::atx-db-modernization-*",
        "arn:aws:s3:::atx-db-modernization-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dms:CreateReplicationSubnetGroup",
        "dms:CreateInstanceProfile",
        "dms:CreateDataProvider",
        "dms:CreateMigrationProject",
        "dms:CreateEndpoint",
        "dms:AddTagsToResource",
        "rds:CreateDBSubnetGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBInstance",
        "rds:AddTagsToResource",
        "dms:CreateReplicationInstance",
        "dms:CreateReplicationTask"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:subgrp:*",
        "arn:aws:dms:*:*:instance-profile:*",
        "arn:aws:dms:*:*:data-provider:*",
        "arn:aws:dms:*:*:migration-project:*",
        "arn:aws:rds:*:*:subgrp:*",
```

```
        "arn:aws:rds:*:*:cluster:*",
        "arn:aws:rds:*:*:db:*",
        "arn:aws:ec2:*:*:vpc-endpoint:*",
        "arn:aws:dms:*:*:endpoint:*",
        "arn:aws:dms:*:*:rep:*",
        "arn:aws:dms:*:*:task:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Project" : "atx-db-modernization",
          "aws:RequestTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dms:ExportMetadataModelAssessment",
        "dms:StartMetadataModelImport",
        "dms:StartMetadataModelConversion",
        "dms:StartMetadataModelExportToTarget",
        "dms:StartMetadataModelExportAsScripts",
        "dms:StartMetadataModelAssessment",
        "dms:StartMetadataModelCreation",
        "dms:UpdateConversionConfiguration",
        "dms:UpdateMigrationProject",
        "dms:AddTagsToResource",
        "dms:ListTagsForResource",
        "dms:DeleteMigrationProject",
        "dms:DeleteEndpoint",
        "dms:UpdateInstanceProfile",
        "dms:UpdateDataProvider",
        "dms:DeleteInstanceProfile",
        "dms:DeleteDataProvider",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:migration-project:*",
        "arn:aws:dms:*:*:instance-profile:*",
        "arn:aws:dms:*:*:data-provider:*",
        "arn:aws:dms:*:*:endpoint:*",
        "arn:aws:secretsmanager:*:*:secret:*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dms:CreateReplicationInstance",
        "dms:DeleteReplicationInstance",
        "dms:ModifyReplicationInstance",
        "dms:RebootReplicationInstance"
      ],
      "Resource" : "arn:aws:dms:*:*:rep:*",
      "Condition" : {
        "StringEquals" : {
          "dms:rep-tag/Project" : "atx-db-modernization",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dms:DeleteReplicationTask",
        "dms:StartReplicationTask",
        "dms:StopReplicationTask",
        "dms:StartReplicationTaskAssessmentRun",
        "dms:CancelReplicationTaskAssessmentRun"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:task:*",
        "arn:aws:dms:*:*:assessment-run:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "dms:task-tag/Project" : "atx-db-modernization",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/dms-vpc-role",
        "arn:aws:iam::*:role/dms-cloudwatch-logs-role",
        "arn:aws:iam::*:role/dms-secrets-manager-role",
        "arn:aws:iam::*:role/dms-s3-access-role",
        "arn:aws:iam::*:role/DMSPremigrationAssessmentS3Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "iam:PassedToService" : [
            "dms.amazonaws.com",
            "dms.*.amazonaws.com",
            "schema-conversion.dms.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

DBModVirtualSource

Deskripsi: Memberikan izin untuk konektor database yang digunakan oleh ATXHelix selama alur kerja modernisasi database offline (DMS-free)

`DBModVirtualSource`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `DBModVirtualSource` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Juli 2026, 23:12 UTC
- Waktu teredit: 06 Juli 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/DBModVirtualSource`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeInternetGateways",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBSubnetGroups",
        "secretsmanager:ListSecrets",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "rds:ModifyDBSubnetGroup",
      "Resource" : "arn:aws:rds:*:*:subgrp:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:EnableHttpEndpoint",
        "rds:DisableHttpEndpoint",
        "rds-data:ExecuteStatement"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:SecretArn" : "arn:aws:secretsmanager:*:
${aws:PrincipalAccount}:secret:*",
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:UpdateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:atx-db-modernization-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:atx-db-modernization-*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Project" : "atx-db-modernization",
          "aws:RequestTag/Owner" : "database-connector",
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetBucketVersioning"
      ],
      "Resource" : [
        "arn:aws:s3:::atx-db-modernization-*",
        "arn:aws:s3:::atx-db-modernization-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBSubnetGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBInstance",
```

```
        "rds:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:subgrp:*",
        "arn:aws:rds:*:*:cluster:*",
        "arn:aws:rds:*:*:db:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Project" : "atx-db-modernization",
          "aws:RequestTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

DeclarativePoliciesEC2Report

Deskripsi: Menyediakan akses ke API read-only yang diperlukan untuk menjalankan Laporan Status Akun Kebijakan Deklaratif EC2.

`DeclarativePoliciesEC2Report`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 30 November 2024, 13:21 UTC
- Waktu teredit: 03 Juli 2026, 10:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DeclarativePoliciesEC2Report`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeclarativePoliciesEC2Report",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRegions",
        "ec2:GetSerialConsoleAccessStatus",
        "ec2:GetInstanceMetadataDefaults",
        "ec2:GetImageBlockPublicAccessState",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetAllowedImagesSettings",
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeAccountVpcEncryptionControl"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

Deskripsi: Izin diperlukan untuk mendukung Amazon Con CloudWatch tributor Insights untuk Amazon DynamoDB.

`DynamoDBCloudWatchContributorInsightsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 15 November 2019, 21:13 UTC
- Waktu teredit: 15 November 2019, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DeleteInsightRules",
        "cloudwatch:PutInsightRule"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    },
    {
      "Action" : [
        "cloudwatch:DescribeInsightRules"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

DynamoDBGlobalTableSettingsManagementServiceRolePolicy

Deskripsi: Izin yang diperlukan oleh DynamoDB untuk mengelola pengaturan replika tabel global

`DynamoDBGlobalTableSettingsManagementServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 15 Oktober 2025, 17:34 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBGlobalTableSettingsManagementServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBActionsNeededToReplicateSettings",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*",
        "arn:aws:autoscaling:*:*:scalingPolicy:*:resource/dynamodb/table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : [
            "dynamodb"
          ]
        }
      }
    },
    {
      "Sid" : "DynamoDBReplicationServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

DynamoDBKinesisReplicationServiceRolePolicy

Deskripsi: Menyedi AWS akan akses DynamoDB ke KinesisDataStreams

`DynamoDBKinesisReplicationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 12 November 2020, 00:43 UTC
- Waktu teredit: 12 November 2020, 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "kinesis.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStream"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

DynamoDBReplicationServiceRolePolicy

Deskripsi: Izin yang diperlukan oleh DynamoDB untuk replikasi data lintas wilayah

`DynamoDBReplicationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 09 November 2017, 23:55 UTC
- Waktu teredit: 08 Januari 2024, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBActionsNeededForSteadyStateReplication",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:UpdateItem",
        "dynamodb:DeleteItem",
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "dynamodb:Scan",
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:UpdateTimeToLive",
        "dynamodb:DescribeLimits",
        "dynamodb:GetResourcePolicy",
        "application-autoscaling:RegisterScalableTarget",
```

```
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DescribeScalingPolicies",
        "account:ListRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBReplicationServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

EC2ApplicationStatusChecksServiceRolePolicy

Deskripsi: Memungkinkan EC2 untuk menemukan dan mengelola sumber daya yang terkait dengan Pemeriksaan Status Aplikasi EC2

`EC2ApplicationStatusChecksServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 27 April 2026, 23:42 UTC
- Waktu teredit: 15 Juli 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2ApplicationStatusChecksServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : [
            "ec2.application-status-checks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
```

```
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Usage"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

EC2FastLaunchFullAccess

Deskripsi: Kebijakan ini memberikan akses penuh ke tindakan Peluncuran Cepat EC2

`EC2FastLaunchFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `EC2FastLaunchFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 Mei 2024, 22:45 UTC
- Waktu teredit: 04 Agustus 2026, 20:27 UTC

- ARN: `arn:aws:iam::aws:policy/EC2FastLaunchFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2FastLaunch",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableFastLaunch",
        "ec2:DisableFastLaunch",
        "ec2:DescribeFastLaunchImages"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeRegions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2CreateVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpc"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2ModifyDeleteVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpc",
        "ec2:CreateSubnet",
        "ec2:ModifyVpcAttribute",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2CreateSubnet",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSubnet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2DeleteSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSubnet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2CreateSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2ManageSecurityGroupEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "CloudFormation",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:RollbackStack",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/EC2FastLaunch*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/EC2FastLaunch*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : "CreateStack"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2LaunchTemplateModify",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyLaunchTemplate",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2LaunchInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Sid" : "EC2LaunchInstanceWithVolAndInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "EC2Tags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Sid" : "EC2ManageTags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ec2fastlaunch.amazonaws.com/
AWSServiceRoleForEC2FastLaunch",
```

```
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMSLRPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:instance-profile/*",
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

EC2FastLaunchServiceRolePolicy

Deskripsi: Kebijakan memberikan ec2fastlaunch untuk menyiapkan dan mengelola snapshot yang telah disediakan sebelumnya di akun pelanggan & mempublikasikan metrik terkait.

`EC2FastLaunchServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 10 Januari 2022, 13:08 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowRunInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
```

```
      ]
    },
    {
      "Sid" : "AllowRunInstancesOnFastLaunchCreatedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStopAndTerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowCreateSnapshot",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowCreateTaggedSnapshot",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "StringLike" : {
          "aws:RequestTag/CreatedByLaunchTemplateVersion" : "*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "CreatedByLaunchTemplateName",
            "CreatedByLaunchTemplateId"
          ]
        }
      }
    },
    {
      "Sid" : "AllowCreateLaunchTemplate",
      "Effect" : "Allow",
      "Action" : "ec2:CreateLaunchTemplate",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowCreateTags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSnapshot",
            "RunInstances",
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Sid" : "AllowDeleteSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowDeleteVolumes",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowDeleteNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeVolumes",
        "ec2:DescribeNetworkInterfaces",
        "cloudformation:DescribeStacks"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPutMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/EC2"
        }
      }
    },
    {
      "Sid" : "AllowEventsRuleMutations",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:PutRule",
        "events:PutTargets"
      ],
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ec2fastlaunch.amazonaws.com"
        }
      },
      "Resource" : [
        "arn:aws:events:*:*:rule/FastLaunch*"
      ]
    },
    {
      "Sid" : "AllowEventsRuleNonMutations",
      "Effect" : "Allow",
      "Action" : [
        "events:ListTargetsByRule",
        "events:DescribeRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/FastLaunch*"
      ]
    },
    {
      "Sid" : "AllowKMSActions",
```

```
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDeleteFastLaunchLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

EC2FleetTimeShiftableServiceRolePolicy

Deskripsi: Kebijakan yang memberikan izin kepada EC2 Fleet untuk meluncurkan instans di masa mendatang.

`EC2FleetTimeShiftableServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran

- Waktu pembuatan: 23 Desember 2019, 19:47 UTC
- Waktu teredit: 23 Desember 2019, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstances",
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:spot-instances-request/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2:fleet-id" : "*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

Ec2ImageBuilderCrossAccountDistributionAccess

Deskripsi: Izin diperlukan oleh EC2 Image Builder untuk melakukan distribusi lintas akun.

`Ec2ImageBuilderCrossAccountDistributionAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `Ec2ImageBuilderCrossAccountDistributionAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 September 2020, 19:22 UTC
- Waktu teredit: 30 September 2020, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/Ec2ImageBuilderCrossAccountDistributionAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*::image/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:CopyImage",
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

EC2ImageBuilderExecutionPolicy

Deskripsi: Memberikan izin yang memungkinkan EC2 Image Builder memanggil AWS layanan atas nama Anda

`EC2ImageBuilderExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `EC2ImageBuilderExecutionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Juni 2026, 17:12 UTC
- Waktu teredit: 08 Juli 2026, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/EC2ImageBuilderExecutionPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RunInstancesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Sid" : "RunInstancesWithEC2ImageBuilderRequestTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Sid" : "IAMPassRolePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "vmie.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EC2InstanceStateChangePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
```

```
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2CopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2CreateImagePermissionsForImage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2CreateImagePermissionsForInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
```

```
      }
    },
    {
      "Sid" : "EC2DeregisterImagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeregisterImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2RegisterImagePermissionsForImage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2RegisterImagePermissionsForSnapshot",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
```

```
        }
      }
    },
    {
      "Sid" : "EC2ModifyImageAttributePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2SnapshotAttributeModificationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ],
```

```
          "ec2:CreateAction" : [
            "CreateImage",
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "CreateCustomerTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:export-image-task/*"
      ]
    },
    {
      "Sid" : "CreateEC2ImageBuilderTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Sid" : "AttachImageWatermarkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachImageWatermark"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "UpdateCustomerLicensePermissions",
      "Effect" : "Allow",
      "Action" : [
        "license-manager:UpdateLicenseSpecificationsForResource"
      ],
      "Resource" : [
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Sid" : "PublishNotificationToCustomerSNSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SystemsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:ListInventoryEntries"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "SystemsManagerPermissionsForAssociation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociationExecutions"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "SystemsManagerPermissionsForInstance",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceAssociationsStatus"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "SendCommandDocumentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunPowerShellScript",
        "arn:aws:ssm:*:*:document/AWS-RunShellScript",
        "arn:aws:ssm:*:*:document/AWSEC2-RunSysprep"
      ]
    },
    {
      "Sid" : "SendCommandEC2ImageBuilderInstancePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
```

```
        }
      }
    },
    {
      "Sid" : "InventoryCollectionAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory"
      ]
    },
    {
      "Sid" : "InventoryCollectionInstancePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "InventoryCollectionTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
```

```
    {
      "Sid" : "DeleteInventoryCollectionAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "EC2KMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:EncryptionContextKeys" : [
            "aws:ebs:id"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EC2KMSDescribeKeyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
```

```
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EC2KMSGrantKeyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountAssumeRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/EC2ImageBuilderDistributionCrossAccountRole"
      ]
    },
    {
      "Sid" : "CloudWatchLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
```

```
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
      ]
    },
    {
      "Sid" : "LaunchTemplatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:ModifyLaunchTemplate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ExportImageBuilderImagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ExportImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "CreateExportImageTaskPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ExportImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:export-image-task/*"
      ]
    },
    {
```

```
      "Sid" : "CancelExportImageTaskPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelExportTask"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:export-image-task/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "CreateSLRForOtherServicesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ssm.amazonaws.com",
            "ec2fastlaunch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EnableFastLaunchPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableFastLaunch"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "ListInspectorFindingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:ListCoverage",
        "inspector2:ListFindings"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateECRImageForInspectorScanningPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/image-builder-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "DeleteECRImageForInspectorScanningPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchDeleteImage"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/image-builder-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
```

```
    {
      "Sid" : "EventBridgePermissionsForInspectorScanning",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/ImageBuilder-*"
      ]
    },
    {
      "Sid" : "ParameterStorePermissionsForImageBuilderParameters",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/imagebuilder/*"
      ]
    },
    {
      "Sid" : "ParameterStorePermissionsForServiceManagedParameters",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*::parameter/aws/service/*"
      ]
    },
    {
      "Sid" : "StartImagePipelineExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:StartImagePipelineExecution",
        "imagebuilder:TagResource"
      ],
      "Resource" : [
        "arn:aws:imagebuilder:*:*:image-pipeline/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

EC2ImageBuilderLifecycleExecutionPolicy

Deskripsi: EC2ImageBuilderLifecycleExecutionPolicy Kebijakan ini memberikan izin kepada Pembuat Gambar untuk melakukan tindakan seperti menghentikan atau menghapus sumber daya gambar Pembuat Gambar dan sumber daya dasarnya (AMI, snapshot) untuk mendukung aturan otomatis untuk tugas manajemen siklus hidup gambar.

`EC2ImageBuilderLifecycleExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `EC2ImageBuilderLifecycleExecutionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 16 November 2023, 23:23 UTC
- Waktu teredit: 16 November 2023, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableImage",
        "ec2:DeregisterImage",
        "ec2:EnableImageDeprecation",
        "ec2:DescribeImageAttribute",
        "ec2:DisableImage",
        "ec2:DisableImageDeprecation"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2DeleteSnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
```

```
      "Sid" : "EC2TagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/DeprecatedBy" : "EC2 Image Builder",
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "DeprecatedBy"
        }
      }
    },
    {
      "Sid" : "ECRImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:BatchDeleteImage"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "StringEquals" : {
          "ecr:ResourceTag/LifecycleExecutionAccess" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "ImageBuilderEC2TagServicePermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "tag:GetResources",
        "imagebuilder:DeleteImage"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

EC2InstanceConnect

Deskripsi: Memungkinkan pelanggan memanggil EC2 Instance Connect untuk menerbitkan kunci sementara ke instans EC2 mereka dan terhubung melalui ssh atau EC2 Instance Connect CLI.

`EC2InstanceConnect`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `EC2InstanceConnect` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2019, 18:53 UTC
- Waktu teredit: 27 Juni 2019, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceConnect`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceConnect",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2-instance-connect:SendSSHPublicKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

Ec2InstanceConnectEndpoint

Deskripsi: Kebijakan titik akhir EC2 Instance Connect untuk mengelola titik akhir EC2 Instance Connect yang dibuat oleh pelanggan

`Ec2InstanceConnectEndpoint`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran

- Waktu pembuatan: 24 Januari 2023, 20:19 UTC
- Waktu teredit: 31 Juli 2025, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
```

```
            "InstanceConnectEndpointId"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "InstanceConnectEndpointId"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:ModifyNetworkInterfaceAttribute",
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

EC2InstanceProfileForImageBuilder

Deskripsi: Profil Instans EC2 untuk layanan Pembuat Gambar.

`EC2InstanceProfileForImageBuilder`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `EC2InstanceProfileForImageBuilder` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2019, 19:08 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot",
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/*.ISO",
        "arn:aws:s3:::*/*.iso",
        "arn:aws:s3:::*/*.Iso"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent",
        "imagebuilder:GetMarketplaceResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:imagebuilder:arn",
          "aws:CalledVia" : [
            "imagebuilder.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::ec2imagebuilder*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

EC2InstanceProfileForImageBuilderECRContainerBuilds

Deskripsi: Profil Instans EC2 untuk membangun gambar kontainer dengan EC2 Image Builder. Kebijakan ini memberikan izin luas kepada pengguna untuk mengunggah gambar ECR.

`EC2InstanceProfileForImageBuilderECRContainerBuilds`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `EC2InstanceProfileForImageBuilderECRContainerBuilds` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Desember 2020, 19:48 UTC
- Waktu teredit: 11 Desember 2020, 19:48 UTC

- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:PutImage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:imagebuilder:arn",
          "aws:CalledVia" : [
```

```
            "imagebuilder.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::ec2imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ECRReplicationServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Replication ECR

`ECRReplicationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 04 Desember 2020, 22:11 UTC
- Waktu teredit: 04 Desember 2020, 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ECRTemplateServiceRolePolicy

Deskripsi: Memungkinkan tindakan dilakukan saat menggunakan templat AWS pembuatan repositori ECR

`ECRTemplateServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 19 Juni 2024, 23:11 UTC
- Waktu teredit: 19 Juni 2024, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRTemplateServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateRepositoryWithTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ElastiCacheServiceRolePolicy

Deskripsi: Kebijakan ini memungkinkan ElastiCache untuk mengelola AWS sumber daya atas nama Anda sebagaimana diperlukan untuk mengelola cache Anda

`ElastiCacheServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 07 Desember 2017, 17:50 UTC
- Waktu teredit: 28 November 2023, 03:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheManagementActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "cloudwatch:PutMetricData",
        "outposts:GetOutpost",
        "outposts:GetOutpostInstanceTypes",
        "outposts:ListOutposts",
        "outposts:ListSites"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDeleteVPCEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
```

```
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
        }
      }
    },
    {
      "Sid" : "TagVPCEndpointsOnCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/AmazonElastiCacheManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonElastiCacheManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAccessToElastiCacheTaggedVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ElasticLoadBalancingFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon ElasticLoadBalancing, dan akses terbatas ke layanan lain yang diperlukan untuk menyediakan ElasticLoadBalancing fitur.

`ElasticLoadBalancingFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ElasticLoadBalancingFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 September 2018, 20:42 UTC
- Waktu teredit: 23 Februari 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeAvailabilityZones",
        "cognito-idp:DescribeUserPoolClient"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "arc-zonal-shift:*",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ElasticLoadBalancingReadOnly

Deskripsi: Menyediakan akses baca saja ke Amazon ElasticLoadBalancing dan layanan dependen

`ElasticLoadBalancingReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ElasticLoadBalancingReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 September 2018, 20:17 UTC
- Waktu teredit: 26 November 2023, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Statement1",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Statement2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Statement3",
      "Effect" : "Allow",
      "Action" : "arc-zonal-shift:GetManagedResource",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
    },
    {
      "Sid" : "Statement4",
      "Effect" : "Allow",
      "Action" : [
        "arc-zonal-shift:ListManagedResources",
```

```
        "arc-zonal-shift:ListZonalShifts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ElementalActivationsDownloadSoftwareAccess

Deskripsi: Akses untuk melihat aset yang dibeli dan mengunduh perangkat lunak terkait dan file kickstart

`ElementalActivationsDownloadSoftwareAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ElementalActivationsDownloadSoftwareAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 September 2020, 17:26 UTC
- Waktu teredit: 08 September 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:Download*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ElementalActivationsFullAccess

Deskripsi: Akses penuh untuk melihat dan mengambil tindakan pada Elemental Appliances dan Perangkat Lunak aset yang dibeli

`ElementalActivationsFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ElementalActivationsFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Juni 2020, 21:00 UTC
- Waktu teredit: 04 Juni 2020, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ElementalActivationsGenerateLicenses

Deskripsi: Akses untuk melihat aset yang dibeli dan menghasilkan lisensi perangkat lunak untuk aktivasi yang tertunda

`ElementalActivationsGenerateLicenses`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ElementalActivationsGenerateLicenses` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Agustus 2020, 18:28 UTC
- Waktu teredit: 28 Agustus 2020 18.28 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ElementalActivationsReadOnlyAccess

Deskripsi: Read-only akses ke daftar terperinci aset yang dibeli terkait dengan pengguna Akun AWS

`ElementalActivationsReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ElementalActivationsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Agustus 2020, 16:51 UTC
- Waktu teredit: 28 Agustus 2020, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ElementalAppliancesSoftwareFullAccess

Deskripsi: Akses penuh untuk melihat dan mengambil tindakan pada Elemental Appliances dan penawaran dan pesanan Perangkat Lunak

`ElementalAppliancesSoftwareFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ElementalAppliancesSoftwareFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 31 Juli 2019, 16:28 UTC

- Waktu teredit: 05 Februari 2021, 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ElementalAppliancesSoftwareReadOnlyAccess

Deskripsi: Read-only akses untuk melihat penawaran dan pesanan Peralatan Elemental dan Perangkat Lunak

`ElementalAppliancesSoftwareReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ElementalAppliancesSoftwareReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 April 2020, 22:31 UTC
- Waktu teredit: 01 April 2020, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:List*",
        "elemental-appliances-software:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ElementalSupportCenterFullAccess

Deskripsi: Akses penuh untuk melihat dan mengambil tindakan pada kasus dukungan Elemental Appliance dan Perangkat Lunak dan konten dukungan produk

`ElementalSupportCenterFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ElementalSupportCenterFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 November 2020, 18:08 UTC
- Waktu teredit: 05 Februari 2021, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-support-cases:*",
        "elemental-support-content:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

EMRDescribeClusterPolicyForEMRWAL

Deskripsi: Kebijakan ini memberikan izin baca-saja yang memungkinkan layanan WAL untuk Amazon EMR menemukan dan mengembalikan status cluster

`EMRDescribeClusterPolicyForEMRWAL`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 15 Juni 2023, 23:30 UTC
- Waktu teredit: 15 Juni 2023, 23:30 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

EndUserMessagingServiceRolePolicy

Deskripsi: Memungkinkan EndUserMessaging untuk mempublikasikan metrik untuk CloudWatch atas nama Anda

`EndUserMessagingServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 29 September 2026, 19:37 UTC
- Waktu teredit: 29 September 2026, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EndUserMessagingServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/EndUserMessaging"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

FinOpsAgentAgentPolicy

Deskripsi: Memberikan izin yang diperlukan oleh AWS FinOps Agen untuk melakukan analisis biaya dan menemukan peluang penghematan biaya pada AWS sumber daya pelanggan.

`FinOpsAgentAgentPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `FinOpsAgentAgentPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Juni 2026, 19:57 UTC
- Waktu teredit: 02 Oktober 2026, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/FinOpsAgentAgentPolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FinOpsAgentDataAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ce:GetCostAndUsage",
        "ce:GetCostAndUsageWithResources",
        "ce:GetCostForecast",
        "ce:GetUsageForecast",
        "ce:GetDimensionValues",
        "ce:GetTags",
        "ce:GetCostCategories",
        "ce:GetCostAndUsageComparisons",
        "ce:GetCostComparisonDrivers",
        "ce:GetSavingsPlansCoverage",
        "ce:GetSavingsPlansUtilization",
        "ce:GetSavingsPlansUtilizationDetails",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "ce:GetReservationCoverage",
        "ce:GetReservationUtilization",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetAnomalies",
        "ce:GetAnomalyMonitors",
        "ce:ListCostAllocationTags",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:DescribeCostCategoryDefinition",
        "ce:ListCostCategoryDefinitions",
        "ce:StartCommitmentPurchaseAnalysis",
        "ce:ListCommitmentPurchaseAnalyses",
        "ce:GetCommitmentPurchaseAnalysis",
        "ce:StartSavingsPlansPurchaseRecommendationGeneration",
        "ce:ListSavingsPlansPurchaseRecommendationGeneration",
        "ce:GetSavingsPlanPurchaseRecommendationDetails",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ViewBudget",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
        "compute-optimizer:DescribeRecommendationExportJobs",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:GetEnrollmentStatusesForOrganization",
        "compute-optimizer:GetRecommendationSummaries",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEC2RecommendationProjectedMetrics",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEBSVolumeRecommendations",
```

```
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetRecommendationPreferences",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetECSServiceRecommendations",
        "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:GetLicenseRecommendations",
        "compute-optimizer:GetRDSDatabaseRecommendations",
        "compute-optimizer:GetRDSDatabaseRecommendationProjectedMetrics",
        "compute-optimizer:GetIdleRecommendations",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ecs:ListServices",
        "ecs:ListClusters",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "lambda:ListFunctions",
        "lambda:ListProvisionedConcurrencyConfigs",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBMajorEngineVersions",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetProducts",
        "freetier:GetFreeTierUsage",
        "bcm-pricing-calculator:GetPreferences",
        "bcm-pricing-calculator:GetWorkloadEstimate",
        "bcm-pricing-calculator:ListWorkloadEstimateUsage",
        "bcm-pricing-calculator:ListWorkloadEstimates",
        "cloudtrail:LookupEvents",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "logs:StartQuery",
        "logs:GetQueryResults",
        "billing:GetBillingView",
        "billing:GetEnterpriseSupportChargeSummary",
        "billing:GetEnterpriseSupportContractDetails",
        "billing:ListBillingViews",
```

```
        "billing:ListEnterpriseSupportLinkedAccountCharges",
        "billing:ListSourceViewsForBillingView",
        "billing:GetResourcePolicy",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroupCostReports",
        "billingconductor:GetBillingGroupCostReport",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListCustomLineItemVersions",
        "billingconductor:ListResourcesAssociatedToCustomLineItem",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListPricingPlansAssociatedWithPricingRule",
        "invoicing:ListInvoiceSummaries",
        "invoicing:ListInvoiceUnits",
        "invoicing:GetInvoiceUnit",
        "invoicing:BatchGetInvoiceProfile",
        "invoicing:ListProcurementPortalPreferences",
        "invoicing:GetProcurementPortalPreference",
        "aco-automation:GetAutomationEvent",
        "aco-automation:GetAutomationRule",
        "aco-automation:GetEnrollmentConfiguration",
        "aco-automation:ListAccounts",
        "aco-automation:ListAutomationEvents",
        "aco-automation:ListAutomationEventSteps",
        "aco-automation:ListAutomationEventSummaries",
        "aco-automation:ListAutomationRules",
        "aco-automation:ListRecommendedActions",
        "aco-automation:ListRecommendedActionSummaries",
        "aco-automation:ListAutomationRulePreview",
        "aco-automation:ListAutomationRulePreviewSummaries",
        "aco-automation:ListTagsForResource",
        "billing:GetCredits",
        "billing:GetCreditAllocationHistory",
        "health:DescribeEvents",
        "savingsplans:DescribeSavingsPlans",
        "savingsplans:DescribeSavingsPlanRates",
        "savingsplans:DescribeSavingsPlansOfferings",
        "savingsplans:DescribeSavingsPlansOfferingRates",
        "savingsplans:ListTagsForResource",
        "cost-optimization-hub:ListEfficiencyMetrics",
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:GetPreferences",
```

```
        "billing:GetBillingPreferences",
        "billing:ListBillingViewSegments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridgeManagedRuleManagementWritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:EnableRule",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "finops-agent.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EventBridgeManagedRuleManagementReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

FinOpsAgentOperatorPolicy

Deskripsi: Menyediakan akses untuk menggunakan aplikasi web AWS FinOps Agen untuk Agen.

`FinOpsAgentOperatorPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `FinOpsAgentOperatorPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Juni 2026, 19:57 UTC
- Waktu teredit: 03 Juni 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/FinOpsAgentOperatorPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "FinOpsAgentOperatorAccess",
      "Effect" : "Allow",
      "Action" : [
        "finops-agent:CreateConversation",
        "finops-agent:ListConversations",
        "finops-agent:CreateTurn",
        "finops-agent:GetTurn",
        "finops-agent:ListTurns",
        "finops-agent:CancelTurn",
        "finops-agent:AcceptAgentRequest",
        "finops-agent:RejectAgentRequest",
        "finops-agent:GetAgentRequest",
        "finops-agent:CreateTask",
        "finops-agent:GetTask",
        "finops-agent:ListTasks",
        "finops-agent:CancelTask",
        "finops-agent:CreateAutomation",
        "finops-agent:GetAutomation",
        "finops-agent:ListAutomations",
        "finops-agent:UpdateAutomation",
        "finops-agent:DeleteAutomation",
        "finops-agent:CreateDocument",
        "finops-agent:GetDocumentContent",
        "finops-agent:GetDocumentMetadata",
        "finops-agent:ListDocuments",
        "finops-agent:UpdateDocument",
        "finops-agent:DeleteDocument",
        "finops-agent:RestoreDocument",
        "finops-agent:GetArtifactContent",
        "finops-agent:GetArtifactMetadata",
        "finops-agent:DeleteArtifact",
        "finops-agent:ListArtifacts",
        "finops-agent:ListRecords",
        "finops-agent:SendFeedback"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

FMSServiceRolePolicy

Deskripsi: Kebijakan akses untuk mengizinkan peran terkait layanan FM untuk melakukan FM-related tindakan pada FM-managed sumber daya dalam akun AWS Organisasi pelanggan.

`FMSServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 28 Maret 2018, 23:01 UTC
- Waktu teredit: 06 April 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v37 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WafGeneral",
```

```
      "Effect" : "Allow",
      "Action" : [
        "waf:UpdateWebACL",
        "waf:DeleteWebACL",
        "waf:GetWebACL",
        "waf:GetRuleGroup",
        "waf:ListSubscribedRuleGroups",
        "waf-regional:UpdateWebACL",
        "waf-regional:DeleteWebACL",
        "waf-regional:GetWebACL",
        "waf-regional:GetRuleGroup",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListResourcesForWebACL",
        "waf-regional:AssociateWebACL",
        "waf-regional:DisassociateWebACL",
        "elasticloadbalancing:SetWebACL",
        "apigateway:SetWebACL",
        "elasticloadbalancing:SetSecurityGroups",
        "waf:ListTagsForResource",
        "waf-regional:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*"
      ]
    },
    {
      "Sid" : "Wafv2Logging",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:ListLoggingConfigurations",
        "wafv2:DeleteLoggingConfiguration"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:regional/webacl/*",
        "arn:aws:wafv2:*:*:global/webacl/*"
      ]
    },
```

```
    {
      "Sid" : "WafWebaclCreation",
      "Effect" : "Allow",
      "Action" : [
        "waf:CreateWebACL",
        "waf-regional:CreateWebACL",
        "waf:GetChangeToken",
        "waf-regional:GetChangeToken",
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:*",
        "arn:aws:waf-regional:*:*:*"
      ]
    },
    {
      "Sid" : "ElbGeneral",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "WafPermissionPolicy",
      "Effect" : "Allow",
      "Action" : [
        "waf:PutPermissionPolicy",
        "waf:GetPermissionPolicy",
        "waf:DeletePermissionPolicy",
        "waf-regional:PutPermissionPolicy",
        "waf-regional:GetPermissionPolicy",
        "waf-regional:DeletePermissionPolicy"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:rulegroup/*"
      ]
    },
    {
      "Sid" : "CloudfrontGeneral",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution",
        "cloudfront:UpdateDistribution",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:ListDistributions",
        "cloudfront:ListTagsForResource",
        "cloudfront:AssociateDistributionWebACL",
        "cloudfront:DisassociateDistributionWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudfrontVpcOriginAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetVpcOrigin"
      ],
      "Resource" : "arn:aws:cloudfront::*:vpcorigin/*"
    },
    {
      "Sid" : "ConfigScoped",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule",
        "config:PutConfigRule",
        "config:StartConfigRulesEvaluation",
        "config:DeleteEvaluationResults"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/fms.amazonaws.com/
*"
    },
    {
      "Sid" : "ConfigUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeComplianceByConfigRule",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRules",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:PutConfigurationRecorder",
        "config:StartConfigurationRecorder",
```

```
        "config:PutDeliveryChannel",
        "config:DescribeDeliveryChannels",
        "config:DescribeDeliveryChannelStatus",
        "config:GetComplianceSummaryByConfigRule",
        "config:GetDiscoveredResourceCounts",
        "config:PutEvaluations",
        "config:SelectResourceConfig",
        "config:BatchGetResourceConfig"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SlrDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/fms.amazonaws.com/AWSServiceRoleForFMS"
      ]
    },
    {
      "Sid" : "OrganizationsGeneral",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListChildren",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ShieldGeneral",
      "Effect" : "Allow",
      "Action" : [
```

```
        "shield:CreateProtection",
        "shield:DeleteProtection",
        "shield:DescribeProtection",
        "shield:ListProtections",
        "shield:ListAttacks",
        "shield:CreateSubscription",
        "shield:DescribeSubscription",
        "shield:GetSubscriptionState",
        "shield:DescribeDRTAccess",
        "shield:DescribeEmergencyContactSettings",
        "shield:UpdateEmergencyContactSettings",
        "elasticloadbalancing:DescribeLoadBalancers",
        "ec2:DescribeAddresses",
        "shield:EnableApplicationLayerAutomaticResponse",
        "shield:DisableApplicationLayerAutomaticResponse",
        "shield:UpdateApplicationLayerAutomaticResponse"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2SecurityGroupScoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "SecurityGroupTagCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid" : "SecurityGroupTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/FMManaged" : "*"
        }
      }
    },
    {
      "Sid" : "Ec2Unscoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeInstances",
        "ec2:AssociateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DisassociateRouteTable",
        "ec2:ReplaceRouteTableAssociation"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Wafv2General",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:TagResource",
        "wafv2:ListResourcesForWebACL",
        "wafv2:AssociateWebACL",
        "wafv2:ListTagsForResource",
        "wafv2:UntagResource",
        "wafv2:GetWebACL",
        "wafv2:DisassociateFirewallManager",
        "wafv2:DeleteWebACL",
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/webacl/*",
        "arn:aws:wafv2:*:*:regional/webacl/*"
      ]
    },
    {
      "Sid" : "Wafv2WebAclAndRuleGroupMutation",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:UpdateWebACL",
        "wafv2:CreateWebACL",
        "wafv2:DeleteFirewallManagerRuleGroups",
        "wafv2:PutFirewallManagerRuleGroups"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/webacl/*",
        "arn:aws:wafv2:*:*:regional/webacl/*",
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*",
        "arn:aws:wafv2:*:*:global/managedruleset/*",
        "arn:aws:wafv2:*:*:regional/managedruleset/*",
        "arn:aws:wafv2:*:*:global/ipset/*",
        "arn:aws:wafv2:*:*:regional/ipset/*",
        "arn:aws:wafv2:*:*:global/regexpatternset/*",
        "arn:aws:wafv2:*:*:regional/regexpatternset/*"
```

```
      ]
    },
    {
      "Sid" : "Wafv2PermissionPolicy",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutPermissionPolicy",
        "wafv2:GetPermissionPolicy",
        "wafv2:DeletePermissionPolicy"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*"
      ]
    },
    {
      "Sid" : "Wafv2WebaclDescribe",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACLForResource"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:regional/webacl/*"
      ]
    },
    {
      "Sid" : "RouteTableTagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateRouteTable"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "SubnetTagManagement",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "VPCEndpointTagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "RouteTableCleanup",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteRouteTable",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/FMManaged" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "Ec2DescribeUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInternetGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateVpcEndpointScoped",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : [
            "true"
          ]
        }
      }
    },
    {
      "Sid" : "CreateVpcEndpointUnscoped",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "VpcEndpointsDeletion",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RamTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:resource-share/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "RamMutation",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RamCreation",
      "Effect" : "Allow",
      "Action" : "ram:CreateResourceShare",
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : [
            "true"
          ]
        }
      }
    },
    {
      "Sid" : "RamDescribe",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SlrCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "network-firewall.amazonaws.com",
            "shield.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamDescribe",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "NetworkFirewallTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "NetworkFirewallGeneral",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:AssociateSubnets",
        "network-firewall:CreateFirewall",
        "network-firewall:CreateFirewallPolicy",
        "network-firewall:DisassociateSubnets",
        "network-firewall:UpdateFirewallDeleteProtection",
        "network-firewall:UpdateFirewallPolicy",
        "network-firewall:UpdateFirewallPolicyChangeProtection",
        "network-firewall:UpdateSubnetChangeProtection",
        "network-firewall:AssociateFirewallPolicy",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DeleteResourcePolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:UpdateLoggingConfiguration",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:ListTLSInspectionConfigurations"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "NetworkFirewallResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:network-firewall:*:*:firewall-policy/*",
        "arn:aws:network-firewall:*:*:stateful-rulegroup/*",
        "arn:aws:network-firewall:*:*:stateless-rulegroup/*"
      ]
    },
    {
      "Sid" : "NetworkFirewallCleanup",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DeleteFirewallPolicy",
        "network-firewall:DeleteFirewall"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LogsGeneral",
      "Effect" : "Allow",
      "Action" : [
        "logs:ListLogDeliveries",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Route53ResolverRuleGroupUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListTagsForResource",
        "route53resolver:ListFirewallRuleGroups",
```

```
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupPolicy",
        "route53resolver:PutFirewallRuleGroupPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Route53ResolverRuleGroupCleanup",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:UpdateFirewallRuleGroupAssociation",
        "route53resolver:DisassociateFirewallRuleGroup"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Route53ResolverRuleGroupScoped",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:AssociateFirewallRuleGroup",
        "route53resolver:TagResource"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NaclTagCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : [
            "Name",
            "FMManaged",
            "FMPolicies"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkAcl"
        }
      }
    },
    {
      "Sid" : "NaclTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged",
            "FMPolicies"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NaclScoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkAclEntry",
        "ec2:CreateNetworkAclEntry",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:DeleteNetworkAcl"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NaclUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:DescribeNetworkAcls",
        "ec2:CreateNetworkAcl"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

FSxDeleteServiceLinkedRoleAccess

Deskripsi: Mengizinkan Amazon FSx menghapus Peran Tertaut Layanan untuk akses Amazon S3

`FSxDeleteServiceLinkedRoleAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 28 November 2018, 10:40 UTC
- Waktu teredit: 28 November 2018, 10:40 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetRole"
      ],
      "Resource" : "arn:*:iam::*:role/aws-service-role/s3.data-
source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

GameLiftContainerFleetPolicy

Deskripsi: Memberikan izin yang diperlukan untuk tindakan komputasi dalam armada GameLift kontainer Amazon, termasuk akses ke dependensi seperti Amazon S3.

`GameLiftContainerFleetPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `GameLiftContainerFleetPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 November 2024, 19:28 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/GameLiftContainerFleetPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WriteGameSessionLogsToLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:gamelift-*:log-stream:*"
    },
    {
      "Sid" : "CreateLogGroupToStoreGameSessionLogs",
      "Effect" : "Allow",
```

```
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:gamelift-*"
    },
    {
      "Sid" : "WriteGameSessionLogsToS3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::gamelift-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RetrieveComputeAuthToken",
      "Effect" : "Allow",
      "Action" : [
        "gamelift:GetComputeAuthToken"
      ],
      "Resource" : [
        "arn:aws:gamelift:*:*:containerfleet/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

GameLiftGameServerGroupPolicy

Deskripsi: Kebijakan untuk mengizinkan Gamelift GameServerGroups mengelola sumber daya pelanggan

`GameLiftGameServerGroupPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `GameLiftGameServerGroupPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 April 2020, 23:12 UTC
- Waktu teredit: 13 Mei 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/GameLift" : "GameServerGroups"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:EnterStandby",
        "autoscaling:SetInstanceProtection",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:SuspendProcesses",
        "autoscaling:DetachInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/GameLift" : "GameServerGroups"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sns:Publish",
      "Resource" : [
        "arn:*:sns:*:*:ActivatingLifecycleHookTopic-*",
        "arn:*:sns:*:*:TerminatingLifecycleHookTopic-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/GameLift"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

GitLabDuoWithAmazonQPermissionsPolicy

Deskripsi: Kebijakan terkelola ini memberikan izin untuk terhubung dengan Amazon Q dan memanfaatkan fitur-fitur di GitLab Duo dengan integrasi Amazon Q.

`GitLabDuoWithAmazonQPermissionsPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `GitLabDuoWithAmazonQPermissionsPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 April 2025, 16:37 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/GitLabDuoWithAmazonQPermissionsPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GitLabDuoUsagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:SendEvent",
        "q:CreateAuthGrant",
        "q:UpdateAuthGrant",
        "q:GenerateCodeRecommendations",
        "q:SendMessage",
        "q:ListPlugins",
        "q:VerifyOAuthAppConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GitLabDuoManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:CreateOAuthAppConnection",
        "q:DeleteOAuthAppConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GitLabDuoPluginPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:CreatePlugin",
        "q:DeletePlugin",
        "q:GetPlugin"
```

```
      ],
      "Resource" : "arn:aws:qdeveloper:*:*:plugin/GitLabDuoWithAmazonQ/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

GlobalAcceleratorFullAccess

Deskripsi: Izinkan GlobalAccelerator Pengguna Akses penuh ke semua API

`GlobalAcceleratorFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `GlobalAcceleratorFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2018, 02:44 UTC
- Waktu teredit: 04 Desember 2020 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "globalaccelerator:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeRegions",
        "ec2:DescribeSubnets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
globalaccelerator.amazonaws.com/AWSServiceRoleForGlobalAccelerator*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "globalaccelerator.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

GlobalAcceleratorReadOnlyAccess

Deskripsi: Izinkan GlobalAccelerator Pengguna Akses ke API Hanya Baca

`GlobalAcceleratorReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `GlobalAcceleratorReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2018, 02:41 UTC
- Waktu teredit: 27 November 2018, 02:41 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Action" : [
        "globalaccelerator:Describe*",
        "globalaccelerator:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

GreengrassOTAUpdateArtifactAccess

Deskripsi: Menyediakan akses baca ke artefak Pembaruan Greengrass OTA di semua wilayah Greengrass

`GreengrassOTAUpdateArtifactAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `GreengrassOTAUpdateArtifactAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 29 November 2017, 18:11 UTC
- Waktu teredit: 18 Desember 2018, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-greengrass-updates/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

GroundTruthSyntheticConsoleFullAccess

Deskripsi: Kebijakan ini memberikan izin yang diperlukan untuk menggunakan semua fitur G SageMaker round Truth Synthetic Console.

`GroundTruthSyntheticConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `GroundTruthSyntheticConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Agustus 2022, 15:58 UTC
- Waktu teredit: 25 Agustus 2022 15.58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

GroundTruthSyntheticConsoleReadOnlyAccess

Deskripsi: Kebijakan ini memberikan akses baca-saja ke G SageMaker round Truth Synthetic melalui. Konsol Manajemen AWS

`GroundTruthSyntheticConsoleReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `GroundTruthSyntheticConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Agustus 2022, 15:58 UTC
- Waktu teredit: 25 Agustus 2022 15.58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

Health_OrganizationsServiceRolePolicy

Deskripsi: Kebijakan AWS kesehatan untuk mengaktifkan fitur Tampilan Organisasi

`Health_OrganizationsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 16 Desember 2019, 13:28 UTC
- Waktu teredit: 06 Februari 2024, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

IAMAccessAdvisorReadOnly

Deskripsi: Kebijakan ini memberikan akses untuk membaca semua informasi akses yang disediakan oleh penasihat akses IAM seperti informasi layanan yang terakhir diakses.

`IAMAccessAdvisorReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `IAMAccessAdvisorReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Juni 2019, 19:33 UTC
- Waktu teredit: 21 Juni 2019, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListPolicies",
        "iam:ListPoliciesGrantingServiceAccess",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:GenerateOrganizationsAccessReport",
        "iam:GenerateCredentialReport",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetServiceLastAccessedDetails",
        "iam:GetServiceLastAccessedDetailsWithEntities",
        "iam:GetOrganizationsAccessReport",
```

```
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListPolicies",
        "organizations:ListTargetsForPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

IAMAccessAnalyzerFullAccess

Deskripsi: Menyediakan akses penuh ke Penganalisis Akses IAM

`IAMAccessAnalyzerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `IAMAccessAnalyzerFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Desember 2019, 17:12 UTC
- Waktu teredit: 02 Desember 2019, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "access-analyzer.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
```

```
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

IAMAccessAnalyzerReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke sumber daya Penganalisis Akses IAM

`IAMAccessAnalyzerReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `IAMAccessAnalyzerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Desember 2019, 17:12 UTC
- Waktu teredit: 18 Juli 2024, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMAccessAnalyzerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CheckAccessNotGranted",
        "access-analyzer:CheckNoNewAccess",
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:Get*",
        "access-analyzer:List*",
        "access-analyzer:ValidatePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```


Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

IAMFullAccess

Deskripsi: Menyediakan akses penuh ke IAM melalui. Konsol Manajemen AWS

`IAMFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `IAMFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 21 Juni 2019, 19:40 UTC
- ARN: `arn:aws:iam::aws:policy/IAMFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:*",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListPolicies",
        "organizations:ListTargetsForPolicy"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

IAMReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke IAM melalui. Konsol Manajemen AWS

`IAMReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `IAMReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu teredit: 25 Januari 2018, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/IAMReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

IAMSelfManageServiceSpecificCredentials

Deskripsi: Mengizinkan pengguna IAM mengelola Kredensi Khusus Layanan mereka sendiri.

`IAMSelfManageServiceSpecificCredentials`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `IAMSelfManageServiceSpecificCredentials` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 Desember 2016, 17:25 UTC
- Waktu teredit: 22 Desember 2016, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:ListServiceSpecificCredentials",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

IAMUserChangePassword

Deskripsi: Menyediakan kemampuan bagi pengguna IAM untuk mengubah kata sandi mereka sendiri.

`IAMUserChangePassword`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `IAMUserChangePassword` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 November 2016, 00:25 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserChangePassword`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ChangePassword"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:user/${aws:username}",
        "arn:aws:iam::*:user/*/${aws:username}"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetAccountPasswordPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

IAMUserSSHKeys

Deskripsi: Menyediakan kemampuan bagi pengguna IAM untuk mengelola kunci SSH mereka sendiri.

`IAMUserSSHKeys`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `IAMUserSSHKeys` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Juli 2015, 17:08 UTC
- Waktu teredit: 09 Juli 2015, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserSSHKeys`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

IVSFullAccess

Deskripsi: Menyediakan akses penuh ke Layanan Video Interaktif (IVS), Juga termasuk izin untuk layanan dependen, diperlukan untuk akses penuh ke konsol ivs.

`IVSFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `IVSFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 Desember 2023, 21:20 UTC
- Waktu teredit: 13 Desember 2023, 21:20 UTC
- ARN: `arn:aws:iam::aws:policy/IVSFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:*",
        "ivschat:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

IVSReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke IVS dan API streaming Low-Latency Real-Time

`IVSReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `IVSReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Desember 2023, 18:00 UTC
- Waktu teredit: 25 September 2026, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/IVSReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "IVSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:BatchGetChannel",
        "ivs:GetAdConfiguration",
        "ivs:GetChannel",
        "ivs:GetComposition",
        "ivs:GetEncoderConfiguration",
        "ivs:GetIngestConfiguration",
        "ivs:GetParticipant",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetPublicKey",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStageSession",
        "ivs:GetStorageConfiguration",
        "ivs:GetStream",
        "ivs:GetStreamSession",
        "ivs:ListAdConfigurations",
        "ivs:ListChannels",
        "ivs:ListCompositions",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListParticipants",
        "ivs:ListParticipantReplicas",
        "ivs:ListParticipantEvents",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStageSessions",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListStreams",
        "ivs:ListStreamSessions",
        "ivs:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

IVSRecordToS3

Deskripsi: Peran Tertaut Layanan untuk melakukan S3 PutObject untuk merekam streaming langsung IVS

`IVSRecordToS3`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 05 Desember 2020, 00:10 UTC
- Waktu teredit: 05 Desember 2020, 00:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

KafkaConnectServiceRolePolicy

Deskripsi: Kebijakan ini memberikan izin kepada Kafka Connect untuk mengelola AWS sumber daya atas nama Anda.

`KafkaConnectServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 07 September 2021, 13:12 UTC
- Waktu teredit: 07 September 2021, 13.12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonMSKConnectManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "AmazonMSKConnectManaged"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonMSKConnectManaged" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

KafkaServiceRolePolicy

Deskripsi: Kebijakan peran terkait layanan IAM untuk Kafka.

`KafkaServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 15 November 2018, 23:31 UTC
- Waktu teredit: 10 November 2025, 23:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:AttachNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeVpcEndpoints",
        "acm-pca:GetCertificateAuthorityCertificate",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
```

```
      "Resource" : "arn:*:ec2:*:*:subnet/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
          "ec2:ResourceTag/ClusterArn" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "secretsmanager:SecretId" : "arn:*:secretsmanager:*:*:secret:AmazonMSK_*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:*:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSMSKManaged" : "true"
```

```
        },
        "StringLike" : {
          "ec2:ResourceTag/ClusterArn" : "*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

KeyspacesCDCServiceRolePolicy

Deskripsi: Memberikan izin yang diperlukan ke Amazon Keyspaces untuk Mengubah Pengambilan Data

`KeyspacesCDCServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 21 Juni 2025, 00:22 UTC
- Waktu teredit: 21 Juni 2025, 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesCDCServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KeyspacesPutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Cassandra"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

KeyspacesReplicationServiceRolePolicy

Deskripsi: Izin yang diperlukan oleh ruang kunci untuk replikasi data lintas wilayah

`KeyspacesReplicationServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 02 Mei 2023, 16:15 UTC
- Waktu teredit: 15 November 2024, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KeyspacesActionsNeededForSteadyStateReplication",
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:Modify",
        "cassandra:Alter",
        "cassandra:ModifyMultiRegionResource",
        "cassandra:SelectMultiRegionResource",
        "cassandra:AlterMultiRegionResource",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CWDeleteAlarmPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:TargetTracking-*"
    },
    {
      "Sid" : "CWDescribeAlarmPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "CWPutMetricAlarmPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:TargetTracking-*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "cloudwatch:AlarmActions" : [
            "arn:aws:autoscaling:*:*:scalingPolicy:*:resource/cassandra/keyspace/*/
table/*:policyName/*:createdBy/*"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

LakeFormationDataAccessServiceRolePolicy

Deskripsi: Kebijakan untuk memberikan akses data sementara ke sumber daya Formasi Danau

`LakeFormationDataAccessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 20 Juni 2019, 20:46 UTC
- Waktu teredit: 06 Februari 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LakeFormationDataAccessServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

LexBotPolicy

Deskripsi: Kebijakan untuk kasus penggunaan AWS Lex Bot

`LexBotPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 17 Februari 2017, 22:18 UTC
- Waktu teredit: 13 November 2019, 22.29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:DetectSentiment"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

LexChannelPolicy

Deskripsi: Kebijakan untuk kasus penggunaan AWS Lex Channel

`LexChannelPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 17 Februari 2017, 23:23 UTC
- Waktu teredit: 17 Februari 2017, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lex:PostText"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

LightsailExportAccess

Deskripsi: Kebijakan peran terkait layanan AWS Lightsail yang memberikan izin untuk mengekspor sumber daya

`LightsailExportAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 28 September 2018, 16:35 UTC
- Waktu teredit: 15 Januari 2022, 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/
AWSServiceRoleForLightsail*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot",
        "ec2:DescribeSnapshots",
        "ec2:CopyImage",
        "ec2:DescribeImages"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccountPublicAccessBlock"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

MediaConnectGatewayInstanceRolePolicy

Deskripsi: Kebijakan ini memberikan izin untuk mendaftarkan Instans MediaConnect Gate MediaConnect way ke Gateway.

`MediaConnectGatewayInstanceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `MediaConnectGatewayInstanceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 Maret 2023, 20:43 UTC
- Waktu teredit: 22 Maret 2023, 20:43 UTC
- ARN: `arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MediaConnectGateway",
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DiscoverGatewayPollEndpoint",
        "mediaconnect:PollGateway",
        "mediaconnect:SubmitGatewayStateChange"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

MediaPackageServiceRolePolicy

Deskripsi: Memungkinkan MediaPackage untuk menerbitkan log ke CloudWatch

`MediaPackageServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 18 September 2020, 17:45 UTC
- Waktu teredit: 18 September 2020, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
```

```
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/MediaPackage/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/MediaPackage/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

MemoryDBServiceRolePolicy

Deskripsi: Kebijakan ini memungkinkan MemoryDB mengelola AWS sumber daya atas nama Anda sebagaimana diperlukan untuk mengelola sumber daya Anda.

`MemoryDBServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 17 Agustus 2021, 22:34 UTC
- Waktu teredit: 01 Desember 2024, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateMemoryDBTagsOnNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonMemoryDBManaged"
          ]
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
```

```
    {
      "Sid" : "DeleteMemoryDBTaggedNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonMemoryDBManaged" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "DescribeEC2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PutCloudWatchMetricData",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "cloudwatch:namespace" : "AWS/MemoryDB"
        }
      }
    },
    {
      "Sid" : "ReplicateMemoryDBMultiRegionClusterData",
      "Effect" : "Allow",
      "Action" : [
        "memorydb:ReplicateMultiRegionClusterData"
      ],
      "Resource" : "arn:aws:memorydb:*:*:cluster/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

MigrationHubDMSAccessServiceRolePolicy

Deskripsi: Kebijakan Layanan Migrasi Database untuk mengambil peran dalam akun pelanggan untuk memanggil Pusat Migrasi

`MigrationHubDMSAccessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 12 Juni 2019, 17:50 UTC
- Waktu teredit: 07 Oktober 2019, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgh:CreateProgressUpdateStream",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:DescribeMigrationTask",
        "mgh:AssociateDiscoveredResource",
        "mgh:ListDiscoveredResources",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:DisassociateDiscoveredResource",
        "mgh:AssociateCreatedArtifact",
        "mgh:NotifyMigrationTaskState",
        "mgh:DisassociateCreatedArtifact",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS/migrationTask/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

MigrationHubServiceRolePolicy

Deskripsi: Mengizinkan Migrasi Hub memanggil Layanan Penemuan Aplikasi atas nama Anda

`MigrationHubServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 12 Juni 2019, 17:22 UTC
- Waktu teredit: 06 Agustus 2020, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
        "discovery:DescribeConfigurations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "dms:AddTagsToResource",
      "Resource" : [
        "arn:aws:dms:*:*:endpoint:*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

MigrationHubSMSAccessServiceRolePolicy

Deskripsi: Kebijakan Layanan Migrasi Server untuk mengambil peran dalam akun pelanggan untuk memanggil Migrasi Hub

`MigrationHubSMSAccessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 12 Juni 2019, 18:30 UTC
- Waktu teredit: 07 Oktober 2019, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgh:CreateProgressUpdateStream",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:DescribeMigrationTask",
        "mgh:AssociateDiscoveredResource",
        "mgh:ListDiscoveredResources",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:DisassociateDiscoveredResource",
        "mgh:AssociateCreatedArtifact",
        "mgh:NotifyMigrationTaskState",
        "mgh:DisassociateCreatedArtifact",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS/migrationTask/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

MonitronServiceRolePolicy

Deskripsi: Kebijakan untuk peran terkait layanan AWS Monitron yang memberikan akses ke sumber daya pelanggan yang diperlukan.

`MonitronServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 02 Mei 2022, 19:22 UTC
- Waktu teredit: 02 Mei 2022 19.22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/monitron/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

MultiPartyApprovalFullAccess

Deskripsi: Menyediakan akses penuh untuk Multi-party persetujuan. Kebijakan ini juga mencakup izin terkait untuk AWS Organisasi dan Identi AWS tas IAM untuk mengelola tim persetujuan dan sumber identitas.

`MultiPartyApprovalFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `MultiPartyApprovalFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Juni 2025, 20:22 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/MultiPartyApprovalFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MpaFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "mpa:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOCreateApplication",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication"
      ],
      "Resource" : [
        "arn:aws:sso:::instance/*",
        "arn:aws:sso::aws:applicationProvider/mpa"
      ]
    },
    {
      "Sid" : "SSOApplicationManagement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeApplication",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationGrant",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationAccessScope",
        "sso:DeleteApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "mpa.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeInstance",
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "sso:ListInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

MultiPartyApprovalReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke Multi-party persetujuan. Kebijakan ini juga mencakup izin baca terkait untuk AWS Organisasi dan Identi AWS tas IAM untuk tim persetujuan dan sumber identitas.

`MultiPartyApprovalReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `MultiPartyApprovalReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Juni 2025, 20:07 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/MultiPartyApprovalReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MpaReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "mpa:Get*",
        "mpa:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOManagementAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeInstance",
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

NeptuneConsoleFullAccess

Deskripsi: Menyediakan akses penuh untuk mengelola Amazon Neptunus menggunakan Konsol Manajemen AWS. Perhatikan bahwa kebijakan ini juga memberikan akses penuh untuk mempublikasikan semua topik SNS dalam akun, izin untuk membuat dan mengedit instans Amazon EC2 dan konfigurasi VPC, izin untuk melihat dan mencantumkan kunci di Amazon KMS, dan akses penuh ke Amazon RDS. Untuk informasi selengkapnya, lihat https://aws.amazon.com/neptune/faqs/.

`NeptuneConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `NeptuneConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Juni 2018, 21:35 UTC
- Waktu teredit: 30 November 2023, 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowNeptuneCreate",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : [
            "graphdb",
            "neptune"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForRDS",
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
```

```
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
```

```
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowOtherDepedentPermissions",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
```

```
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "iam:ListRoles",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForNeptune",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "rds.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "AllowCreateSLRForNeptune",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForNeptuneAnalytics",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:CreateGraph",
        "neptune-graph:DeleteGraph",
        "neptune-graph:GetGraph",
        "neptune-graph:ListGraphs",
        "neptune-graph:UpdateGraph",
        "neptune-graph:ResetGraph",
        "neptune-graph:CreateGraphSnapshot",
        "neptune-graph:DeleteGraphSnapshot",
        "neptune-graph:GetGraphSnapshot",
        "neptune-graph:ListGraphSnapshots",
        "neptune-graph:RestoreGraphFromSnapshot",
        "neptune-graph:CreatePrivateGraphEndpoint",
        "neptune-graph:GetPrivateGraphEndpoint",
        "neptune-graph:ListPrivateGraphEndpoints",
        "neptune-graph:DeletePrivateGraphEndpoint",
        "neptune-graph:CreateGraphUsingImportTask",
        "neptune-graph:GetImportTask",
        "neptune-graph:ListImportTasks",
        "neptune-graph:CancelImportTask"
      ],
      "Resource" : [
        "arn:aws:neptune-graph:*:*:*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForNeptuneAnalytics",
```

```
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "neptune-graph.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateSLRForNeptuneAnalytics",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "neptune-graph.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

NeptuneFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Neptunus. Perhatikan bahwa kebijakan ini juga memberikan akses penuh untuk mempublikasikan semua topik SNS dalam akun dan akses penuh ke Amazon RDS. Untuk informasi selengkapnya, lihat https://aws.amazon.com/neptune/faqs/.

`NeptuneFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `NeptuneFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Mei 2018, 19:17 UTC
- Waktu teredit: 22 Januari 2024, 16:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowNeptuneCreate",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : [
            "graphdb",
            "neptune"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBClusterEndpoint",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:CreateGlobalCluster",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterEndpoint",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DeleteGlobalCluster",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
```

```
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:FailoverGlobalCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterEndpoint",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:ModifyGlobalCluster",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveFromGlobalCluster",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime",
        "rds:StartDBCluster",
        "rds:StopDBCluster"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowOtherDepedentPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForNeptune",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateSLRForNeptune",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "AllowDataAccessForNeptune",
      "Effect" : "Allow",
      "Action" : [
        "neptune-db:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

NeptuneGraphReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke semua sumber daya Amazon Neptune Analytics bersama dengan izin baca saja untuk layanan dependen.

`NeptuneGraphReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `NeptuneGraphReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2023, 07:32 UTC
- Waktu teredit: 30 November 2023, 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyPermissionsForNeptuneGraph",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:Get*",
        "neptune-graph:List*",
        "neptune-graph:Read*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForCloudwatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

NeptuneReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Amazon Neptunus. Perhatikan bahwa kebijakan ini juga memberikan akses ke sumber daya Amazon RDS. Untuk informasi selengkapnya, lihat https://aws.amazon.com/neptune/faqs/.

`NeptuneReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `NeptuneReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Mei 2018, 19:16 UTC
- Waktu teredit: 22 Januari 2024, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyPermissionsForRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
```

```
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForCloudwatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "kms:ListAliases",
        "kms:ListKeyPolicies"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ]
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForNeptuneDB",
      "Effect" : "Allow",
      "Action" : [
        "neptune-db:Read*",
        "neptune-db:Get*",
        "neptune-db:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

NetworkAdministrator

Deskripsi: Memberikan izin akses penuh ke AWS layanan dan tindakan yang diperlukan untuk mengatur dan mengonfigurasi sumber daya AWS jaringan.

`NetworkAdministrator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `NetworkAdministrator` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan fungsi pekerjaan
- Waktu pembuatan: 10 November 2016, 17:31 UTC
- Waktu teredit: 09 Juli 2026, 14:42 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/NetworkAdministrator`

Versi kebijakan

Versi kebijakan: v16 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDefaultNetworkAdminActions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudfront:ListDistributions",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "directconnect:*",
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
```

```
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:CreateCarrierGateway",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateFlowLogs",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreatePlacementGroup",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpcEndpointConnectionNotification",
        "ec2:CreateVpcEndpointServiceConfiguration",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteCarrierGateway",
        "ec2:DeleteEgressOnlyInternetGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
```

```
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpointConnectionNotifications",
        "ec2:DeleteVpcEndpointServiceConfigurations",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePrefixLists",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
```

```
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DetachInternetGateway",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:GetVpnConnectionDeviceSampleConfiguration",
        "ec2:GetVpnConnectionDeviceTypes",
        "ec2:GetVpnTunnelReplacementStatus",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySecurityGroupRules",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ModifyVpcEndpointConnectionNotification",
        "ec2:ModifyVpcEndpointServiceConfiguration",
        "ec2:ModifyVpcEndpointServicePermissions",
        "ec2:ModifyVpcPeeringConnectionOptions",
        "ec2:ModifyVpcTenancy",
        "ec2:ModifyVpnConnection",
        "ec2:ModifyVpnConnectionOptions",
        "ec2:ModifyVpnTunnelCertificate",
        "ec2:ModifyVpnTunnelOptions",
        "ec2:MoveAddressToVpc",
        "ec2:RejectVpcEndpointConnections",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:ReplaceVpnTunnel",
        "ec2:ResetNetworkInterfaceAttribute",
        "ec2:RestoreAddressToClassic",
        "ec2:UnassignIpv6Addresses",
```

```
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticloadbalancing:*",
        "interconnect:AcceptConnectionProposal",
        "interconnect:CreateConnection",
        "interconnect:DeleteConnection",
        "interconnect:DescribeConnectionProposal",
        "interconnect:GetConnection",
        "interconnect:GetEnvironment",
        "interconnect:ListAttachPoints",
        "interconnect:ListConnections",
        "interconnect:ListEnvironments",
        "interconnect:ListTagsForResource",
        "interconnect:TagResource",
        "interconnect:UntagResource",
        "interconnect:UpdateConnection",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "route53:*",
        "route53domains:*",
        "sns:CreateTopic",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowVPCPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AssociateSecurityGroupVpc",
        "ec2:AttachClassicLinkVpc",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateVpcPeeringConnection",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
```

```
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DetachClassicLinkVpc",
        "ec2:DisableVpcClassicLink",
        "ec2:DisassociateSecurityGroupVpc",
        "ec2:EnableVpcClassicLink",
        "ec2:GetConsoleScreenshot",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:RejectVpcPeeringConnection",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowLocalGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLocalGatewayRoute",
        "ec2:CreateLocalGatewayRouteTableVpcAssociation",
        "ec2:DeleteLocalGatewayRoute",
        "ec2:DeleteLocalGatewayRouteTableVpcAssociation",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeLocalGateways",
        "ec2:SearchLocalGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DiscoverBuckets",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "s3:ListBucket"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DiscoverFlowLogRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/flow-logs-*"
    },
    {
      "Sid" : "NetworkmanagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TransitGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptTransitGatewayVpcAttachment",
        "ec2:AssociateTransitGatewayRouteTable",
        "ec2:CreateTransitGateway",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayVpcAttachment",
        "ec2:DeleteTransitGateway",
        "ec2:DeleteTransitGatewayRoute",
        "ec2:DeleteTransitGatewayRouteTable",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
```

```
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DisableTransitGatewayRouteTablePropagation",
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:ExportTransitGatewayRoutes",
        "ec2:GetTransitGatewayAttachmentPropagations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:ModifyTransitGateway",
        "ec2:ModifyTransitGatewayVpcAttachment",
        "ec2:RejectTransitGatewayVpcAttachment",
        "ec2:ReplaceTransitGatewayRoute",
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowTransitGatewaySLRCreation",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "transitgateway.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

NetworkSecurityDirectorServiceLinkedRolePolicy

Deskripsi: Memberikan izin untuk peran terkait layanan direktur keamanan jaringan AWS Shield untuk menilai lingkungan tertentu.

`NetworkSecurityDirectorServiceLinkedRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 13 Juni 2025, 20:07 UTC
- Waktu teredit: 24 September 2026, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/NetworkSecurityDirectorServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceLevelPermissionNotSupported",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeAvailabilityZones",
```

```
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetManagedPrefixListEntries",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "wafv2:ListWebACLs",
        "cloudfront:ListDistributions",
        "cloudfront:ListTagsForResource",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "cloudfront",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudfront:GetDistribution"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid" : "classicWaf",
      "Effect" : "Allow",
      "Action" : [
        "waf:ListWebACLs",
        "waf:GetWebACL"
      ],
      "Resource" : [
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf-regional:*:*:webacl/*"
      ]
    },
    {
      "Sid" : "wafv2",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:ListResourcesForWebACL",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:GetRuleGroup",
        "wafv2:DescribeManagedRuleGroup",
        "wafv2:GetWebACL"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*",
        "arn:aws:wafv2:*:*:global/managedruleset/*",
        "arn:aws:wafv2:*:*:regional/managedruleset/*",
        "arn:aws:wafv2:*:*:global/webacl/*/*",
        "arn:aws:wafv2:*:*:regional/webacl/*/*",
        "arn:aws:apprunner:*:*:service/*",
        "arn:aws:cognito-idp:*:*:userpool/*",
        "arn:aws:ec2:*:*:verified-access-instance/*"
      ]
    },
    {
      "Sid" : "directconnect",
      "Effect" : "Allow",
      "Action" : [
```

```
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeVirtualGateways"
      ],
      "Resource" : [
        "arn:aws:directconnect::*:dx-gateway/*",
        "arn:aws:directconnect:*:*:dxcon/*",
        "arn:aws:directconnect:*:*:dxlag/*",
        "arn:aws:directconnect:*:*:dxvif/*"
      ]
    },
    {
      "Sid" : "ec2Get",
      "Effect" : "Allow",
      "Action" : [
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway-route-table/*"
      ]
    },
    {
      "Sid" : "networkFirewall",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:ListFirewalls",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListRuleGroups",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeRuleGroup"
      ],
      "Resource" : [
        "arn:aws:network-firewall:*:*:*/*"
      ]
    },
    {
      "Sid" : "apiGatewayGetAPI",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
```

```
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/tags/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "AllowOrganizationsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListTargetsForPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrganizationsAdmins",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "network-security-director.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "AllowAccountInformationRead",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetRegionOptStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowConfigRecorderList",
      "Effect" : "Allow",
      "Action" : [
        "config:ListConfigurationRecorders"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowConfigRecorderScopedAccess",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "config:ConfigurationRecorderServicePrincipal" : [
            "network-security-director.amazonaws.com"
          ]
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "DisableNSDPolicyType",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DisablePolicyType"
      ],
      "Resource" : "arn:aws:organizations::*:root/o-*/r-*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : "NETWORK_SECURITY_DIRECTOR_POLICY"
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

NetworkSecurityManagerServiceRolePolicy

Deskripsi: Kebijakan akses untuk mengi NetworkSecurityManager zinkan peran terkait layanan untuk melakukan NetworkSecurityManager-related tindakan pada NetworkSecurityManager-managed sumber daya dalam pelanggan Akun AWS.

`NetworkSecurityManagerServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 18 Agustus 2026, 18:27 UTC
- Waktu teredit: 18 Agustus 2026, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/NetworkSecurityManagerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LogsGeneral",
      "Effect" : "Allow",
      "Action" : [
        "logs:ListLogDeliveries",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3LogBucketGeneral",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::aws-waf-logs-*"
    },
    {
      "Sid" : "CloudfrontVpcOriginAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetVpcOrigin"
      ],
      "Resource" : "arn:aws:cloudfront::*:vpcorigin/*"
    },
    {
      "Sid" : "ConfigUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "config:SelectResourceConfig"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeOrganizationUnScoped",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeAccountScoped",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeAccount",
      "Resource" : "arn:aws:organizations::*:account/o-*/*"
    },
    {
      "Sid" : "DescribeOrganizationUnitScoped",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganizationalUnit",
      "Resource" : "arn:aws:organizations::*:ou/o-*/ou-*"
    },
    {
      "Sid" : "ListDelegatedAdministratorsScoped",
      "Effect" : "Allow",
      "Action" : "organizations:ListDelegatedAdministrators",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "network-security-manager.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LoadBalancerNonMutationApiAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeWebACLAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LoadBalancerGetWebACLScoped",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:GetLoadBalancerWebACL",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "CloudFrontDistributionNonMutationApiAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListTagsForResource"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid" : "ApiGatewayStageNonMutationApiAccess",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/tags/*"
      ]
    },
    {
      "Sid" : "Wafv2General",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:TagResource",
        "wafv2:ListResourcesForWebACL",
        "wafv2:AssociateWebACL",
        "wafv2:ListTagsForResource",
        "wafv2:UntagResource",
```

```
        "wafv2:GetWebACL",
        "wafv2:DisassociateFirewallManager",
        "wafv2:DeleteWebACL",
        "wafv2:DisassociateWebACL",
        "wafv2:ValidateNetworkSecurityManagerWebACLConfiguration",
        "wafv2:ValidateNetworkSecurityManagerRuleConfiguration"
      ],
      "Resource" : "arn:aws:wafv2:*:*:*/webacl/*"
    },
    {
      "Sid" : "Wafv2WebAclAndRuleGroupMutation",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:UpdateWebACL",
        "wafv2:CreateWebACL",
        "wafv2:DeleteFirewallManagerRuleGroups",
        "wafv2:PutFirewallManagerRuleGroups"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*",
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*",
        "arn:aws:wafv2:*:*:global/managedruleset/*",
        "arn:aws:wafv2:*:*:regional/managedruleset/*",
        "arn:aws:wafv2:*:*:global/ipset/*",
        "arn:aws:wafv2:*:*:regional/ipset/*",
        "arn:aws:wafv2:*:*:global/regexpatternset/*",
        "arn:aws:wafv2:*:*:regional/regexpatternset/*"
      ]
    },
    {
      "Sid" : "Wafv2Logging",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:DeleteLoggingConfiguration"
      ],
      "Resource" : "arn:aws:wafv2:*:*:*/webacl/*"
    },
    {
      "Sid" : "Wafv2ListLogging",
      "Effect" : "Allow",
      "Action" : "wafv2:ListLoggingConfigurations",
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "Wafv2ListWebACLs",
      "Effect" : "Allow",
      "Action" : "wafv2:ListWebACLs",
      "Resource" : "*"
    },
    {
      "Sid" : "Wafv2PermissionPolicy",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutPermissionPolicy",
        "wafv2:GetPermissionPolicy",
        "wafv2:DeletePermissionPolicy"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*"
      ]
    },
    {
      "Sid" : "Wafv2WebaclDescribe",
      "Effect" : "Allow",
      "Action" : "wafv2:GetWebACLForResource",
      "Resource" : "arn:aws:wafv2:*:*:*/webacl/*"
    },
    {
      "Sid" : "CloudFrontListDistributions",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:ListDistributions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFrontDistributionMutation",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:AssociateDistributionWebACL",
        "cloudfront:DisassociateDistributionWebACL"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution/*"
```

```
    },
    {
      "Sid" : "ElbWebAclRemediationScoped",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateWebACLAssociation",
        "elasticloadbalancing:DeleteWebACLAssociation"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "ElbSetWebAcl",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:SetWebACL",
      "Resource" : "*"
    },
    {
      "Sid" : "ApiGatewayWebAclRemediation",
      "Effect" : "Allow",
      "Action" : "apigateway:SetWebACL",
      "Resource" : "arn:aws:apigateway:*::/restapis/*/stages/*"
    },
    {
      "Sid" : "CognitoWebAclIntegration",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:GetWebACLForResource",
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AppRunnerWebAclIntegration",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:DescribeWebAclForService",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VerifiedAccessWebAclIntegration",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AppSyncWebAclIntegration",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetWebACLForResource",
        "appsync:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifyWebAclIntegration",
      "Effect" : "Allow",
      "Action" : [
        "amplify:GetWebACLForResource",
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ShieldGeneral",
      "Effect" : "Allow",
      "Action" : [
        "shield:CreateProtection",
        "shield:DeleteProtection",
        "shield:DescribeProtection",
        "shield:ListProtections",
        "shield:CreateSubscription",
        "shield:DescribeSubscription",
        "shield:GetSubscriptionState",
        "ec2:DescribeAddresses",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ShieldSlrCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/shield.amazonaws.com/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "shield.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowConfigRecorderList",
      "Effect" : "Allow",
      "Action" : "config:ListConfigurationRecorders",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPutServiceLinkedConfigRecorder",
      "Effect" : "Allow",
      "Action" : "config:PutServiceLinkedConfigurationRecorder",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowConfigRecorderScopedAccess",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:AssociateResourceTypes",
        "config:DisassociateResourceTypes"
      ],
      "Resource" : "arn:aws:config:*:*:configuration-recorder/*"
    },
    {
      "Sid" : "AllowCreateConfigServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowListActionsForAgentCoreGateway",
```

```
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayGetWebACLForResource"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:gateway/*"
    },
    {
      "Sid" : "WafV2LoggingSlrCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/wafv2.amazonaws.com/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "wafv2.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

NovaActServiceRolePolicy

Deskripsi: Kebijakan ini memungkinkan NovaAct untuk membuat dan mengelola sumber daya yang diperlukan untuk mengoperasikan agen Nova Act.

`NovaActServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 26 November 2025, 16:19 UTC
- Waktu teredit: 26 November 2025, 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/NovaActServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPublishCloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/NovaAct"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

OAMFullAccess

Deskripsi: Menyediakan akses penuh ke Pengel CloudWatch ola Akses Observabilitas

`OAMFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `OAMFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2022, 13:38 UTC
- Waktu teredit: 27 November 2022 13.38 UTC
- ARN: `arn:aws:iam::aws:policy/OAMFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

OAMReadOnlyAccess

Deskripsi: Menyediakan akses Baca Saja ke Pengel CloudWatch ola Akses Observabilitas

`OAMReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `OAMReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2022, 13:29 UTC
- Waktu teredit: 27 November 2022 13.29 UTC
- ARN: `arn:aws:iam::aws:policy/OAMReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:Get*",
        "oam:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

OpensearchIngestionSelfManagedVpcePolicy

Deskripsi: Mengizinkan Amazon OpenSearch Ingestion untuk menjelaskan sumber daya jaringan dan menulis metrik layanan ke cloudwatch

`OpensearchIngestionSelfManagedVpcePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 10 Juni 2024, 19:59 UTC
- Waktu teredit: 10 Juni 2024, 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/OpensearchIngestionSelfManagedVpcePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CwPermissionsForOsiNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/OSIS"
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

PartnerCentralAccountManagementUserRoleAssociation

Deskripsi: Menyediakan akses untuk mengasosiasikan dan memisahkan pengguna pusat mitra dengan peran IAM

`PartnerCentralAccountManagementUserRoleAssociation`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `PartnerCentralAccountManagementUserRoleAssociation` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 November 2023, 02:03 UTC
- Waktu teredit: 10 November 2023, 02:03 UTC
- ARN: `arn:aws:iam::aws:policy/PartnerCentralAccountManagementUserRoleAssociation`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PassPartnerCentralRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/PartnerCentralRoleFor*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "partnercentral-account-management.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PartnerUserRoleAssociation",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "partnercentral-account-management:AssociatePartnerUser",
        "partnercentral-account-management:DisassociatePartnerUser"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

PartnerCentralIncentiveBenefitManagement

Deskripsi: Kebijakan menyediakan akses untuk mengelola semua manfaat insentif di Pusat AWS Mitra.

`PartnerCentralIncentiveBenefitManagement`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `PartnerCentralIncentiveBenefitManagement` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Februari 2026, 16:42 UTC
- Waktu teredit: 12 Maret 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/PartnerCentralIncentiveBenefitManagement`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BenefitsManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListBenefits",
        "partnercentral:GetBenefit",
        "partnercentral:CreateBenefitApplication",
        "partnercentral:AmendBenefitApplication",
```

```
        "partnercentral:UpdateBenefitApplication",
        "partnercentral:SubmitBenefitApplication",
        "partnercentral:GetBenefitApplication",
        "partnercentral:CancelBenefitApplication",
        "partnercentral:RecallBenefitApplication",
        "partnercentral:ListBenefitApplications",
        "partnercentral:AssociateBenefitApplicationResource",
        "partnercentral:DisassociateBenefitApplicationResource",
        "partnercentral:ListBenefitAllocations",
        "partnercentral:GetBenefitAllocation"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/benefit-application/*",
        "arn:aws:partnercentral:*:*:catalog/*/benefit-allocation/*",
        "arn:aws:partnercentral:*:*:catalog/*/benefit/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerCentralBenefitsTaggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:TagResource",
        "partnercentral:UntagResource",
        "partnercentral:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/benefit-application/*",
        "arn:aws:partnercentral:*:*:catalog/*/benefit-allocation/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "PartnerResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners",
        "partnercentral:GetPartner"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/partner/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "AWSPartnerOpportunityAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetAwsOpportunitySummary",
        "partnercentral:GetOpportunity",
        "partnercentral:ListOpportunities"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/opportunity/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "ListingAWSMarketplaceEntities",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AWSMarketplaceOffersAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Solution/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/OfferSet/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Offer/*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceAgreementsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:DescribeAgreement"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerCentralEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-
files/${aws:PrincipalAccount}/*"
    },
    {
      "Sid" : "PartnerCentralAgentsSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:UseSession"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        },
        "Bool" : {
          "aws:IsMcpServiceAction" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

PowerUserAccess

Deskripsi: Menyediakan akses penuh ke AWS layanan dan sumber daya, tetapi tidak mengizinkan pengelolaan Pengguna dan grup.

`PowerUserAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `PowerUserAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC

- ARN: `arn:aws:iam::aws:policy/PowerUserAccess`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "NotAction" : [
        "iam:*",
        "organizations:*",
        "account:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetGovCloudAccountInformation",
        "account:GetPrimaryEmail",
        "account:ListRegions",
        "iam:CreateServiceLinkedRole",
        "iam:DeleteServiceLinkedRole",
        "iam:ListRoles",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

PricingPlanManagerFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Pricing Plan Manager

`PricingPlanManagerFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `PricingPlanManagerFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Juli 2026, 16:42 UTC
- Waktu teredit: 30 Juli 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/PricingPlanManagerFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "ppmglobalactions",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:GetSubscription",
        "pricingplanmanager:ListSubscriptions",
        "pricingplanmanager:CreateSubscription",
        "pricingplanmanager:ApprovePaidSubscription",
        "pricingplanmanager:UpdateSubscription",
        "pricingplanmanager:CancelSubscription",
        "pricingplanmanager:CancelSubscriptionChange",
        "pricingplanmanager:AssociateResourcesToSubscription",
        "pricingplanmanager:DisassociateResourcesFromSubscription",
        "freetier:GetAccountPlanState",
        "cloudwatch:GetMetricData",
        "shield:ListProtections"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

PricingPlanManagerReadonlyAccess

Deskripsi: Menyediakan akses baca saja ke Manajer Rencana AWS Harga

`PricingPlanManagerReadonlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `PricingPlanManagerReadonlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Juli 2026, 16:42 UTC
- Waktu teredit: 30 Juli 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/PricingPlanManagerReadonlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ppmglobalactions",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:ListSubscriptions",
        "pricingplanmanager:GetSubscription"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

QAppsServiceRolePolicy

Deskripsi: Memberikan izin ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Amazon Q Apps.

`QAppsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 26 September 2024, 19:22 UTC
- Waktu teredit: 26 September 2024, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/QAppsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QAppsPutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/QApps"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

QBusinessQuicksightPluginPolicy

Deskripsi: Memberikan izin kepada QBusiness untuk memang QuickSight gil API untuk plugin QuickSight

`QBusinessQuicksightPluginPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `QBusinessQuicksightPluginPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Desember 2024, 15:36 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/QBusinessQuicksightPluginPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QBusinessToQuickSightPredictQAResultsInvocation",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:PredictQAResults"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:topic/*",
        "arn:aws:quicksight:*:*:dashboard/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

QBusinessServiceRolePolicy

Deskripsi: Memberikan izin ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Amazon Q

`QBusinessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 29 April 2024, 16:05 UTC
- Waktu teredit: 29 April 2024, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/QBusinessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QBusinessPutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/QBusiness"
        }
      }
    },
    {
      "Sid" : "QBusinessCreateLogGroupPermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/qbusiness/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QBusinessDescribeLogGroupsPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QBusinessLogStreamPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/qbusiness/*:log-stream:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

Deskripsi: Kebijakan yang digunakan oleh QuickSight tim untuk mengakses data pelanggan yang dihasilkan oleh S3 Storage Management Analytics.

`QuickSightAccessForS3StorageManagementAnalyticsReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `QuickSightAccessForS3StorageManagementAnalyticsReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 12 Juni 2017, 18:18 UTC
- Waktu teredit: 08 Oktober 2019, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::s3-analytics-export-shared-*"
      ]
    },
    {
      "Action" : [
        "s3:GetAnalyticsConfiguration",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

RDSCloudHsmAuthorizationRole

Deskripsi: Kebijakan default untuk peran layanan Amazon RDS.

`RDSCloudHsmAuthorizationRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `RDSCloudHsmAuthorizationRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 26 September 2019, 22:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm:DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke AWS layanan dan sumber daya.

`ReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu teredit: 24 September 2026, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v190 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "ReadOnlyActionsGroup1",
      "Effect" : "Allow",
      "Action" : [
        "a4b:Get*",
        "a4b:List*",
        "a4b:Search*",
        "access-analyzer:GetAccessPreview",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
        "access-analyzer:GetFindingsStatistics",
        "access-analyzer:GetGeneratedPolicy",
        "access-analyzer:ListAccessPreviewFindings",
        "access-analyzer:ListAccessPreviews",
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListPolicyGenerations",
        "access-analyzer:ListTagsForResource",
        "access-analyzer:ValidatePolicy",
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:GetGovCloudAccountInformation",
        "account:GetPrimaryEmail",
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "acm-pca:Describe*",
        "acm-pca:Get*",
        "acm-pca:List*",
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "acm:SearchCertificates",
        "action-recommendations:ListRecommendedActions",
        "agent-registry:GetDiscoverableRegistryRecord",
        "agent-registry:GetRegistry",
        "agent-registry:GetRegistryRecord",
        "agent-registry:InvokeRegistryMcp",
        "agent-registry:ListDiscoverableRegistryRecords",
        "agent-registry:ListRegistries",
        "agent-registry:ListRegistryRecords",
```

```
        "agent-registry:ListTagsForResource",
        "agent-registry:SearchDiscoverableRegistryRecords",
        "aidevops:DescribePrivateConnection",
        "aidevops:DescribeServices",
        "aidevops:GetAccountUsage",
        "aidevops:GetAgentSpace",
        "aidevops:GetAssociation",
        "aidevops:GetBacklogTask",
        "aidevops:GetKnowledgeItem",
        "aidevops:GetOperatorApp",
        "aidevops:GetRecommendation",
        "aidevops:GetService",
        "aidevops:ListAgentSpaces",
        "aidevops:ListAssociations",
        "aidevops:ListBacklogTasks",
        "aidevops:ListChats",
        "aidevops:ListExecutions",
        "aidevops:ListGoals",
        "aidevops:ListJournalRecords",
        "aidevops:ListKnowledgeItems",
        "aidevops:ListKnowledgeItemVersions",
        "aidevops:ListPendingMessages",
        "aidevops:ListPrivateConnections",
        "aidevops:ListRecommendations",
        "aidevops:ListServices",
        "aidevops:ListTagsForResource",
        "aidevops:ListWebhooks",
        "aidevops:SearchServiceAccessibleResource",
        "aiops:GetEphemeralInvestigationResults",
        "aiops:GetFact",
        "aiops:GetFactVersions",
        "aiops:GetInvestigation",
        "aiops:GetInvestigationEvent",
        "aiops:GetInvestigationGroup",
        "aiops:GetInvestigationResource",
        "aiops:GetReport",
        "aiops:ListFacts",
        "aiops:ListInvestigationEvents",
        "aiops:ListInvestigationGroups",
        "aiops:ListInvestigations",
        "aiops:ValidateInvestigationGroup",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
```

```
        "amplify:GetBackendEnvironment",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:GetJob",
        "amplify:GetWebhook",
        "amplify:ListApps",
        "amplify:ListArtifacts",
        "amplify:ListBackendEnvironments",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListJobs",
        "amplify:ListTagsForResource",
        "amplify:ListWebhooks",
        "aoss:BatchGetCollection",
        "aoss:BatchGetCollectionGroup",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetAccountSettings",
        "aoss:GetPoliciesStats",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollectionGroups",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListTagsForResource",
        "aoss:ListVpcEndpoints",
        "apigateway:GET",
        "apigateway:GetPortal",
        "apigateway:GetPortalProduct",
        "apigateway:GetProductPage",
        "apigateway:GetProductRestEndpointPage",
        "apigateway:GetRoutingRule",
        "apigateway:ListPortalProducts",
        "apigateway:ListPortals",
        "apigateway:ListProductPages",
        "apigateway:ListProductRestEndpointPages",
        "apigateway:ListRoutingRules",
        "apigateway:GetPortalProductSharingPolicy",
        "appconfig:GetApplication",
        "appconfig:GetConfiguration",
```

```
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExtension",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensions",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appconfig:GetAccountSettings",
        "appconfig:GetExperimentDefinition",
        "appconfig:GetExperimentRun",
        "appconfig:GetExtensionAssociation",
        "appconfig:ListExperimentDefinitions",
        "appconfig:ListExperimentRunEvents",
        "appconfig:ListExperimentRuns",
        "appconfig:ListExtensionAssociations",
        "appfabric:GetAppAuthorization",
        "appfabric:GetAppBundle",
        "appfabric:GetIngestion",
        "appfabric:GetIngestionDestination",
        "appfabric:ListAppAuthorizations",
        "appfabric:ListAppBundles",
        "appfabric:ListIngestionDestinations",
        "appfabric:ListIngestions",
        "appfabric:ListTagsForResource",
        "appflow:DescribeConnector",
        "appflow:DescribeConnectorEntity",
        "appflow:DescribeConnectorFields",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeConnectors",
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecution",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:DescribeFlows",
        "appflow:ListConnectorEntities",
        "appflow:ListConnectorFields",
        "appflow:ListConnectors",
        "appflow:ListFlows",
```

```
        "appflow:ListTagsForResource",
        "application-autoscaling:Describe*",
        "application-autoscaling:GetPredictiveScalingForecast",
        "application-autoscaling:ListTagsForResource",
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListAuditFindings",
        "application-signals:ListEntityEvents",
        "application-signals:ListGroupingAttributeDefinitions",
        "application-signals:ListObservedEntities",
        "application-signals:ListServiceDependencies",
        "application-signals:ListServiceDependents",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServiceOperations",
        "application-signals:ListServices",
        "application-signals:ListServiceStates",
        "application-signals:ListTagsForResource",
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "appmesh:Describe*",
        "appmesh:List*",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeCustomDomains",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:DescribeWebAclForService",
        "apprunner:ListAssociatedServicesForWebAcl",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListOperations",
        "apprunner:ListServices",
        "apprunner:ListServicesForAutoScalingConfiguration",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appstream:Describe*",
        "appstream:List*",
        "appstudio:GetAccountStatus",
        "appstudio:GetEnablementJobStatus",
```

```
        "appsync:Get*",
        "appsync:List*",
        "appsync:EvaluateMappingTemplate",
        "apptest:GetTestCase",
        "apptest:GetTestConfiguration",
        "apptest:GetTestRunStep",
        "apptest:GetTestSuite",
        "apptest:ListTagsForResource",
        "apptest:ListTestCases",
        "apptest:ListTestConfigurations",
        "apptest:ListTestRuns",
        "apptest:ListTestRunSteps",
        "apptest:ListTestRunTestCases",
        "apptest:ListTestSuites",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeAnomalyDetector",
        "aps:DescribeLoggingConfiguration",
        "aps:DescribeQueryLoggingConfiguration",
        "aps:DescribeResourcePolicy",
        "aps:DescribeRuleGroupsNamespace",
        "aps:DescribeScraper",
        "aps:DescribeScraperLoggingConfiguration",
        "aps:DescribeWorkspace",
        "aps:DescribeWorkspaceConfiguration",
        "aps:GetAlertManagerSilence",
        "aps:GetAlertManagerStatus",
        "aps:GetDefaultScraperConfiguration",
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:ListAlertManagerAlertGroups",
        "aps:ListAlertManagerAlerts",
        "aps:ListAlertManagerReceivers",
        "aps:ListAlertManagerSilences",
        "aps:ListAlerts",
        "aps:ListAnomalyDetectors",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListRules",
        "aps:ListScrapers",
        "aps:ListTagsForResource",
        "aps:ListWorkspaces",
        "aps:PreviewAnomalyDetector",
        "aps:QueryMetrics",
        "arc-region-switch:GetPlan",
```

```
        "arc-region-switch:GetPlanEvaluationStatus",
        "arc-region-switch:GetPlanExecution",
        "arc-region-switch:GetPlanInRegion",
        "arc-region-switch:ListPlanExecutionEvents",
        "arc-region-switch:ListPlanExecutions",
        "arc-region-switch:ListPlans",
        "arc-region-switch:ListPlansInRegion",
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListRoute53HealthChecksInRegion",
        "arc-region-switch:ListTagsForResource",
        "arc-zonal-shift:GetAutoshiftObserverNotificationStatus",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:ListAutoshifts",
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts",
        "artifact:GetCustomerAgreement",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements",
        "artifact:ListReports",
        "artifact:ListReportVersions",
        "athena:Batch*",
        "athena:Get*",
        "athena:List*",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:GetAssessmentFramework",
        "auditmanager:GetAssessmentReportUrl",
        "auditmanager:GetChangeLogs",
        "auditmanager:GetControl",
        "auditmanager:GetDelegations",
        "auditmanager:GetEvidence",
        "auditmanager:GetEvidenceByEvidenceFolder",
        "auditmanager:GetEvidenceFolder",
        "auditmanager:GetEvidenceFoldersByAssessment",
        "auditmanager:GetEvidenceFoldersByAssessmentControl",
        "auditmanager:GetOrganizationAdminAccount",
        "auditmanager:GetServicesInScope",
        "auditmanager:GetSettings",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessmentReports",
        "auditmanager:ListAssessments",
```

```
        "auditmanager:ListControls",
        "auditmanager:ListKeywordsForDataSource",
        "auditmanager:ListNotifications",
        "auditmanager:ListTagsForResource",
        "auditmanager:ValidateAssessmentReportIntegrity",
        "autoscaling-plans:Describe*",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:Describe*",
        "autoscaling:GetPredictiveScalingForecast",
        "aws-portal:View*",
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway",
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings",
        "backup-gateway:GetVirtualMachine",
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:Describe*",
        "backup:Get*",
        "backup:List*",
        "batch:Describe*",
        "batch:List*",
        "bedrock-agentcore:GetABTest",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetApiKeyCredentialProvider",
        "bedrock-agentcore:GetBatchEvaluation",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetBrowserProfile",
        "bedrock-agentcore:GetBrowserSession",
        "bedrock-agentcore:GetCapacityProvider",
        "bedrock-agentcore:GetCodeInterpreter",
        "bedrock-agentcore:GetCodeInterpreterSession",
        "bedrock-agentcore:GetConfigurationBundle",
        "bedrock-agentcore:GetConfigurationBundleVersion",
        "bedrock-agentcore:GetEvaluator",
        "bedrock-agentcore:GetEvent",
        "bedrock-agentcore:GetGateway",
        "bedrock-agentcore:GetGatewayTarget",
        "bedrock-agentcore:GetHarness",
        "bedrock-agentcore:GetHarnessEndpoint",
        "bedrock-agentcore:GetMemory",
```

```
        "bedrock-agentcore:GetMemoryRecord",
        "bedrock-agentcore:GetOauth2CredentialProvider",
        "bedrock-agentcore:GetOnlineEvaluationConfig",
        "bedrock-agentcore:GetPolicy",
        "bedrock-agentcore:GetPolicyEngine",
        "bedrock-agentcore:GetPolicyGeneration",
        "bedrock-agentcore:GetRecommendation",
        "bedrock-agentcore:GetTokenVault",
        "bedrock-agentcore:GetWorkloadIdentity",
        "bedrock-agentcore:ListAgentRuntimeVersionsByCapacityProvider",
        "bedrock-agentcore:ListCapacityProviders",
        "bedrock-agentcore:ListABTests",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListAgentRuntimeVersions",
        "bedrock-agentcore:ListApiKeyCredentialProviders",
        "bedrock-agentcore:ListBatchEvaluations",
        "bedrock-agentcore:ListBrowserProfiles",
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListBrowserSessions",
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListCodeInterpreterSessions",
        "bedrock-agentcore:ListConfigurationBundles",
        "bedrock-agentcore:ListConfigurationBundleVersions",
        "bedrock-agentcore:ListEvaluators",
        "bedrock-agentcore:ListEvents",
        "bedrock-agentcore:ListGateways",
        "bedrock-agentcore:ListGatewayTargets",
        "bedrock-agentcore:ListHarnesses",
        "bedrock-agentcore:ListHarnessEndpoints",
        "bedrock-agentcore:ListMemories",
        "bedrock-agentcore:ListMemoryRecords",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "bedrock-agentcore:ListOnlineEvaluationConfigs",
        "bedrock-agentcore:ListPolicies",
        "bedrock-agentcore:ListPolicyEngines",
        "bedrock-agentcore:ListPolicyGenerationAssets",
        "bedrock-agentcore:ListPolicyGenerations",
        "bedrock-agentcore:ListRecommendations",
        "bedrock-agentcore:ListTagsForResource",
        "bedrock-agentcore:ListWorkloadIdentities",
        "bedrock-agentcore:RetrieveMemoryRecords",
        "bedrock-agentcore:GetPolicyEngineSummary",
        "bedrock-agentcore:GetPolicyGenerationSummary",
```

```
        "bedrock-agentcore:GetPolicySummary",
        "bedrock-agentcore:ListPolicyEngineSummaries",
        "bedrock-agentcore:ListPolicyGenerationSummaries",
        "bedrock-agentcore:ListPolicySummaries",
        "bedrock-agentcore:GetResourcePolicy",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:GetCustomModel",
        "bedrock:GetDataSource",
        "bedrock:GetEvaluationJob",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetIngestionJob",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetPrompt",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:GetResourcePolicy",
        "bedrock:GetUseCaseForModelAccess",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListAgentVersions",
        "bedrock:ListCustomModels",
        "bedrock:ListDataSources",
        "bedrock:ListEnforcedGuardrailsConfiguration",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlows",
        "bedrock:ListFlowVersions",
        "bedrock:ListFoundationModelAgreementOffers",
```

```
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListIngestionJobs",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListModelCustomizationJobs",
        "bedrock:ListModelInvocationJobs",
        "bedrock:ListPrompts",
        "bedrock:ListProvisionedModelThroughputs",
        "bedrock:AgenticRetrieveStream",
        "bedrock:CheckIngestedDocumentAcl",
        "bedrock:CountTokens",
        "bedrock:GetAccountDataRetention",
        "bedrock:GetAdvancedPromptOptimizationJob",
        "bedrock:GetAgentMemory",
        "bedrock:GetAsyncInvoke",
        "bedrock:GetAutomatedReasoningPolicy",
        "bedrock:GetAutomatedReasoningPolicyAnnotations",
        "bedrock:GetAutomatedReasoningPolicyBuildWorkflow",
        "bedrock:GetAutomatedReasoningPolicyBuildWorkflowResultAssets",
        "bedrock:GetAutomatedReasoningPolicyNextScenario",
        "bedrock:GetAutomatedReasoningPolicyTestCase",
        "bedrock:GetAutomatedReasoningPolicyTestResult",
        "bedrock:GetBlueprint",
        "bedrock:GetBlueprintOptimizationStatus",
        "bedrock:GetBlueprintRecommendation",
        "bedrock:GetCustomModelDeployment",
        "bedrock:GetDataAutomationLibrary",
        "bedrock:GetDataAutomationLibraryEntity",
        "bedrock:GetDataAutomationLibraryIngestionJob",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataAutomationStatus",
        "bedrock:GetDocumentContent",
        "bedrock:GetExecutionFlowSnapshot",
        "bedrock:GetFlowExecution",
        "bedrock:GetImportedModel",
        "bedrock:GetIngestedDocumentAcl",
        "bedrock:GetInvocationStep",
        "bedrock:GetInvoke",
        "bedrock:GetKnowledgeBaseDocuments",
        "bedrock:GetMarketplaceModelEndpoint",
        "bedrock:GetModelCopyJob",
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:GetCustomizedModel",
```

```
        "bedrock-mantle:GetFile",
        "bedrock-mantle:GetFineTuningJob",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:GetProject",
        "bedrock-mantle:GetReservation",
        "bedrock-mantle:ListCustomizedModelAssociations",
        "bedrock-mantle:ListCustomizedModels",
        "bedrock-mantle:ListFiles",
        "bedrock-mantle:ListFineTuningJobs",
        "bedrock-mantle:ListModels",
        "bedrock-mantle:ListProjects",
        "bedrock-mantle:ListReservations",
        "bedrock-mantle:ListTagsForResource",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetBillingView",
        "billing:GetCreditAllocationHistory",
        "billing:GetContractInformation",
        "billing:GetCredits",
        "billing:GetIAMAccessPreference",
        "billing:GetResourcePolicy",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "billing:ListSourceViewsForBillingView",
        "billing:ListTagsForResource",
        "billingconductor:GetBillingGroupCostReport",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroupCostReports",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListCustomLineItemVersions",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingPlansAssociatedWithPricingRule",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListResourcesAssociatedToCustomLineItem",
        "billingconductor:ListTagsForResource",
        "braket:GetDevice",
        "braket:GetJob",
        "braket:GetQuantumTask",
        "braket:SearchDevices",
```

```
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "braket:SearchSpendingLimits",
        "budgets:Describe*",
        "budgets:ListTagsForResource",
        "budgets:View*",
        "cassandra:Select",
        "ce:DescribeCostCategoryDefinition",
        "ce:DescribeNotificationSubscription",
        "ce:DescribeReport",
        "ce:GetAnomalies",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:GetApproximateUsageRecords",
        "ce:GetCommitmentPurchaseAnalysis",
        "ce:GetCostAndUsage",
        "ce:GetCostAndUsageComparisons",
        "ce:GetCostAndUsageWithResources",
        "ce:GetCostCategories",
        "ce:GetCostComparisonDrivers",
        "ce:GetCostForecast",
        "ce:GetDimensionValues",
        "ce:GetPreferences",
        "ce:GetReservationCoverage",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetReservationUtilization",
        "ce:GetRightsizingRecommendation",
        "ce:GetSavingsPlanPurchaseRecommendationDetails",
        "ce:GetSavingsPlansCoverage",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "ce:GetSavingsPlansUtilization",
        "ce:GetSavingsPlansUtilizationDetails",
        "ce:GetTags",
        "ce:GetUsageForecast",
        "ce:ListCommitmentPurchaseAnalyses",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:ListCostAllocationTags",
        "ce:ListCostCategoryDefinitions",
        "ce:ListCostCategoryResourceAssociations",
        "ce:ListSavingsPlansPurchaseRecommendationGeneration",
        "ce:ListTagsForResource",
        "chatbot:Describe*",
        "chatbot:Get*",
        "chatbot:List*",
```

```
        "chime:Get*",
        "chime:List*",
        "chime:Retrieve*",
        "chime:Search*",
        "chime:Validate*",
        "cleanrooms-ml:GetAudienceGenerationJob",
        "cleanrooms-ml:GetAudienceModel",
        "cleanrooms-ml:GetConfiguredAudienceModel",
        "cleanrooms-ml:GetConfiguredAudienceModelPolicy",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListAudienceExportJobs",
        "cleanrooms-ml:ListAudienceGenerationJobs",
        "cleanrooms-ml:ListAudienceModels",
        "cleanrooms-ml:ListConfiguredAudienceModels",
        "cleanrooms-ml:ListTagsForResource",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaborationChangeRequest",
        "cleanrooms:GetCollaborationConfiguredAudienceModelAssociation",
        "cleanrooms:GetCollaborationIdNamespaceAssociation",
        "cleanrooms:GetCollaborationPrivacyBudgetTemplate",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetConfiguredTableAssociationAnalysisRule",
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:GetProtectedJob",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationChangeRequests",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborationIdNamespaceAssociations",
```

```
        "cleanrooms:ListCollaborationPrivacyBudgets",
        "cleanrooms:ListCollaborationPrivacyBudgetTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredAudienceModelAssociations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgets",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListProtectedJobs",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:PreviewPrivacyImpact",
        "cloud9:Describe*",
        "cloud9:List*",
        "clouddirectory:BatchRead",
        "clouddirectory:Get*",
        "clouddirectory:List*",
        "clouddirectory:LookupPolicy",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:Describe*",
        "cloudformation:Detect*",
        "cloudformation:Estimate*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "cloudfront-keyvaluestore:Describe*",
        "cloudfront-keyvaluestore:Get*",
        "cloudfront-keyvaluestore:List*",
        "cloudfront:Describe*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudhsm:Describe*",
        "cloudhsm:GetResourcePolicy",
        "cloudhsm:List*",
        "cloudsearch:Describe*",
        "cloudsearch:List*",
        "cloudtrail:Describe*",
        "cloudtrail:Get*",
        "cloudtrail:List*",
```

```
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GenerateQueryResultsSummary",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackage",
        "codeartifact:DescribePackageVersion",
        "codeartifact:DescribeRepository",
        "codeartifact:GetAuthorizationToken",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetPackageVersionAsset",
        "codeartifact:GetPackageVersionReadme",
        "codeartifact:GetRepositoryEndpoint",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersionAssets",
        "codeartifact:ListPackageVersionDependencies",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListRepositoriesInDomain",
        "codeartifact:ListTagsForResource",
        "codeartifact:ReadFromRepository",
        "codebuild:BatchGet*",
        "codebuild:DescribeCodeCoverages",
        "codebuild:DescribeTestCases",
        "codebuild:List*",
        "codecatalyst:GetBillingAuthorization",
        "codecatalyst:GetConnection",
        "codecatalyst:GetPendingConnection",
        "codecatalyst:ListConnections",
        "codecatalyst:ListIamRolesForConnection",
        "codecatalyst:ListTagsForResource",
        "codecommit:BatchGet*",
        "codecommit:Describe*",
        "codecommit:Get*",
        "codecommit:GitPull",
        "codecommit:List*",
        "codeconnections:GetConnection",
        "codeconnections:GetHost",
        "codeconnections:GetRepositoryLink",
        "codeconnections:GetRepositorySyncStatus",
```

```
        "codeconnections:GetResourceSyncStatus",
        "codeconnections:GetSyncConfiguration",
        "codeconnections:ListConnections",
        "codeconnections:ListHosts",
        "codeconnections:ListRepositoryLinks",
        "codeconnections:ListRepositorySyncDefinitions",
        "codeconnections:ListSyncConfigurations",
        "codeconnections:ListTagsForResource",
        "codedeploy:BatchGet*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:Get*",
        "codeguru-profiler:List*",
        "codeguru-reviewer:Describe*",
        "codeguru-reviewer:Get*",
        "codeguru-reviewer:List*",
        "codepipeline:Get*",
        "codepipeline:List*",
        "codestar-connections:GetConnection",
        "codestar-connections:GetHost",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:GetRepositorySyncStatus",
        "codestar-connections:GetResourceSyncStatus",
        "codestar-connections:GetSyncConfiguration",
        "codestar-connections:ListConnections",
        "codestar-connections:ListHosts",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListRepositorySyncDefinitions",
        "codestar-connections:ListSyncConfigurations",
        "codestar-connections:ListTagsForResource",
        "codestar-notifications:describeNotificationRule",
        "codestar-notifications:listEventTypes",
        "codestar-notifications:listNotificationRules",
        "codestar-notifications:listTagsForResource",
        "codestar-notifications:ListTargets",
        "codestar:Describe*",
        "codestar:Get*",
        "codestar:List*",
        "codestar:Verify*",
        "codewhisperer:ListProfiles",
        "cognito-identity:Describe*",
        "cognito-identity:GetCredentialsForIdentity",
        "cognito-identity:GetIdentityPoolAnalytics",
```

```
        "cognito-identity:GetIdentityPoolDailyAnalytics",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetIdentityProviderDailyAnalytics",
        "cognito-identity:GetOpenIdToken",
        "cognito-identity:GetOpenIdTokenForDeveloperIdentity",
        "cognito-identity:List*",
        "cognito-identity:Lookup*",
        "cognito-idp:AdminGet*",
        "cognito-idp:AdminList*",
        "cognito-idp:Describe*",
        "cognito-idp:Get*",
        "cognito-idp:List*",
        "cognito-sync:Describe*",
        "cognito-sync:Get*",
        "cognito-sync:List*",
        "cognito-sync:QueryRecords",
        "comprehend:BatchDetect*",
        "comprehend:Classify*",
        "comprehend:Contains*",
        "comprehend:Describe*",
        "comprehend:Detect*",
        "comprehend:List*",
        "compute-optimizer:DescribeRecommendationExportJobs",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEBSVolumeRecommendations",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEC2RecommendationProjectedMetrics",
        "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:GetECSServiceRecommendations",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:GetEnrollmentStatusesForOrganization",
        "compute-optimizer:GetIdleRecommendations",
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetLicenseRecommendations",
        "compute-optimizer:GetRDSDatabaseRecommendationProjectedMetrics",
        "compute-optimizer:GetRDSDatabaseRecommendations",
        "compute-optimizer:GetRecommendationPreferences",
        "compute-optimizer:GetRecommendationSummaries",
        "config:BatchGetAggregateResourceConfig",
        "config:BatchGetResourceConfig",
        "config:Deliver*",
        "config:Describe*",
        "config:Get*",
```

```
        "config:List*",
        "config:SelectAggregateResourceConfig",
        "config:SelectResourceConfig",
        "connect:Describe*",
        "connect:GetContactAttributes",
        "connect:GetCurrentMetricData",
        "connect:GetCurrentUserData",
        "connect:GetFederationToken",
        "connect:GetMetricData",
        "connect:GetMetricDataV2",
        "connect:GetTaskTemplate",
        "connect:GetTrafficDistribution",
        "connect:List*",
        "consoleapp:GetDeviceIdentity",
        "consoleapp:ListDeviceIdentities",
        "consolidatedbilling:GetAccountBillingRole",
        "consolidatedbilling:ListLinkedAccounts",
        "controlcatalog:GetControl",
        "controlcatalog:ListCommonControls",
        "controlcatalog:ListControlMappings",
        "controlcatalog:ListControls",
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListEfficiencyMetrics",
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "customer-verification:GetCustomerVerificationDetails",
        "customer-verification:GetCustomerVerificationEligibility",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeJobRun",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobRuns",
        "databrew:ListJobs",
```

```
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "databrew:ListTagsForResource",
        "dataexchange:Get*",
        "dataexchange:List*",
        "datapipeline:Describe*",
        "datapipeline:EvaluateExpression",
        "datapipeline:Get*",
        "datapipeline:List*",
        "datapipeline:QueryObjects",
        "datapipeline:Validate*",
        "datasync:Describe*",
        "datasync:List*",
        "datazone:GetAsset",
        "datazone:GetAssetType",
        "datazone:GetDataProduct",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetDomainSharingPolicy",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetLineageNode",
        "datazone:GetListing",
        "datazone:GetMetadataGenerationRun",
        "datazone:GetProject",
        "datazone:GetProjectProfile",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetTimeSeriesDataPoint",
```

```
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetRevisions",
        "datazone:ListDataProductRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListDomains",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListLineageNodeHistory",
        "datazone:ListNotifications",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjectProfiles",
        "datazone:ListProjects",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptions",
        "datazone:ListSubscriptionTargets",
        "datazone:ListTagsForResource",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "dax:BatchGetItem",
        "dax:Describe*",
        "dax:GetItem",
        "dax:ListTags",
        "dax:Query",
        "dax:Scan",
        "deadline:BatchGetJobEntity",
        "deadline:GetApplicationVersion",
        "deadline:GetBudget",
        "deadline:GetFarm",
```

```
        "deadline:GetFleet",
        "deadline:GetJob",
        "deadline:GetLicenseEndpoint",
        "deadline:GetLimit",
        "deadline:GetMonitor",
        "deadline:GetMonitorSettings",
        "deadline:GetQueue",
        "deadline:GetQueueLimitAssociation",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetSessionsStatisticsAggregation",
        "deadline:GetStep",
        "deadline:GetStorageProfile",
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",
        "deadline:GetVolume",
        "deadline:GetWorker",
        "deadline:ListAvailableMeteredProducts",
        "deadline:ListBudgets",
        "deadline:ListFarmMembers",
        "deadline:ListFarms",
        "deadline:ListFleetMembers",
        "deadline:ListFleets",
        "deadline:ListJobMembers",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListJobs",
        "deadline:ListLicenseEndpoints",
        "deadline:ListLimits",
        "deadline:ListMeteredProducts",
        "deadline:ListMonitors",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListQueueLimitAssociations",
        "deadline:ListQueueMembers",
        "deadline:ListQueues",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListSessionsForWorker",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListStorageProfiles",
```

```
        "deadline:ListStorageProfilesForQueue",
        "deadline:ListTagsForResource",
        "deadline:ListTasks",
        "deadline:ListVolumes",
        "deadline:ListWorkers",
        "deadline:SearchJobs",
        "deadline:SearchSteps",
        "deadline:SearchTasks",
        "deadline:SearchWorkers",
        "deepcomposer:GetComposition",
        "deepcomposer:GetModel",
        "deepcomposer:GetSampleModel",
        "deepcomposer:ListCompositions",
        "deepcomposer:ListModels",
        "deepcomposer:ListSampleModels",
        "deepcomposer:ListTrainingTopics",
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:Get*",
        "detective:List*",
        "detective:SearchGraph",
        "devicefarm:Get*",
        "devicefarm:List*",
        "devops-guru:DescribeAccountHealth",
        "devops-guru:DescribeAccountOverview",
        "devops-guru:DescribeAnomaly",
        "devops-guru:DescribeEventSourcesConfig",
        "devops-guru:DescribeFeedback",
        "devops-guru:DescribeInsight",
        "devops-guru:DescribeOrganizationHealth",
        "devops-guru:DescribeOrganizationOverview",
        "devops-guru:DescribeOrganizationResourceCollectionHealth",
        "devops-guru:DescribeResourceCollectionHealth",
        "devops-guru:DescribeServiceIntegration",
        "devops-guru:GetCostEstimation",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListAnomaliesForInsight",
        "devops-guru:ListAnomalousLogGroups",
        "devops-guru:ListEvents",
        "devops-guru:ListInsights",
        "devops-guru:ListMonitoredResources",
        "devops-guru:ListNotificationChannels",
        "devops-guru:ListOrganizationInsights",
        "devops-guru:ListRecommendations",
```

```
        "devops-guru:SearchInsights",
        "devops-guru:StartCostEstimation",
        "directconnect:Describe*",
        "directconnect:ListVirtualInterfaceRoutes",
        "directconnect:ListVirtualInterfaceTestHistory",
        "directconnect:GetResiliencyGroup",
        "directconnect:ListResiliencyGroupAssociations",
        "directconnect:ListResiliencyGroups",
        "discovery:Describe*",
        "discovery:Get*",
        "discovery:List*",
        "dlm:Get*",
        "dlm:ListTagsForResource",
        "dms:Describe*",
        "dms:List*",
        "dms:Test*",
        "docdb-elastic:GetCluster",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:ListClusters",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:ListPendingMaintenanceActions",
        "docdb-elastic:ListTagsForResource",
        "drs:DescribeJobLogItems",
        "drs:DescribeJobs",
        "drs:DescribeLaunchConfigurationTemplates",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeRecoverySnapshots",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:DescribeSourceNetworks",
        "drs:DescribeSourceServers",
        "drs:GetFailbackReplicationConfiguration",
        "drs:GetLaunchConfiguration",
        "drs:GetReplicationConfiguration",
        "drs:ListExtensibleSourceServers",
        "drs:ListLaunchActions",
        "drs:ListStagingAccounts",
        "drs:ListTagsForResource",
        "ds:Check*",
        "ds:Describe*",
        "ds:Get*",
        "ds:List*",
        "ds:Verify*",
        "dsql:GetCluster",
        "dsql:GetClusterPolicy",
```

```
        "dsql:GetStream",
        "dsql:GetVpcEndpointServiceName",
        "dsql:ListClusters",
        "dsql:ListStreams",
        "dsql:ListTagsForResource",
        "dynamodb:BatchGet*",
        "dynamodb:Describe*",
        "dynamodb:Get*",
        "dynamodb:List*",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dynamodb:ReadDataForReplication",
        "dynamodb:SearchVectors",
        "ec2:Describe*",
        "ec2:DescribeInstanceImageMetadata",
        "ec2:Get*",
        "ec2:ListImagesInRecycleBin",
        "ec2:ListSnapshotsInRecycleBin",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:ListVolumesInRecycleBin",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2messages:Get*",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetAuthorizationToken",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchCheck*",
        "ecr:BatchGet*",
        "ecr:Describe*",
        "ecr:Get*",
        "ecr:List*",
        "ecs:Describe*",
        "ecs:GetTaskProtection",
        "ecs:List*",
        "eks:AccessKubernetesApi",
        "eks:Describe*",
```

```
        "eks:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:Request*",
        "elasticbeanstalk:Retrieve*",
        "elasticbeanstalk:Validate*",
        "elasticfilesystem:Describe*",
        "elasticfilesystem:ListTagsForResource",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:List*",
        "elasticmapreduce:View*",
        "elastictranscoder:List*",
        "elastictranscoder:Read*",
        "elemental-appliances-software:Get*",
        "elemental-appliances-software:List*",
        "elemental-inference:ExportDictionaryEntries",
        "elemental-inference:GetDictionary",
        "elemental-inference:GetFeed",
        "elemental-inference:ListDictionaries",
        "elemental-inference:ListFeeds",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "emr-serverless:ListTagsForResource",
        "es:Describe*",
        "es:ESHttpGet",
        "es:ESHttpHead",
        "es:Get*",
        "es:List*",
        "events:Describe*",
```

```
        "events:List*",
        "events:Test*",
        "evidently:GetExperiment",
        "evidently:GetExperimentResults",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegmentReferences",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "evidently:TestSegmentPattern",
        "firehose:Describe*",
        "firehose:List*",
        "fis:GetAction",
        "fis:GetExperiment",
        "fis:GetExperimentTargetAccountConfiguration",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:GetTargetResourceType",
        "fis:ListActions",
        "fis:ListExperimentResolvedTargets",
        "fis:ListExperiments",
        "fis:ListExperimentTargetAccountConfigurations",
        "fis:ListExperimentTemplates",
        "fis:ListTagsForResource",
        "fis:ListTargetAccountConfigurations",
        "fis:ListTargetResourceTypes",
        "fms:GetAdminAccount",
        "fms:GetAdminScope",
        "fms:GetAppsList",
        "fms:GetComplianceDetail",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:GetProtectionStatus",
        "fms:GetProtocolsList",
        "fms:GetViolationDetails",
        "fms:ListAppsLists",
        "fms:ListComplianceStatus",
        "fms:ListMemberAccounts",
```

```
        "fms:ListPolicies",
        "fms:ListProtocolsLists",
        "fms:ListTagsForResource",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeExplainability",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribeMonitor",
        "forecast:DescribePredictor",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:DescribeWhatIfAnalysis",
        "forecast:DescribeWhatIfForecast",
        "forecast:DescribeWhatIfForecastExport",
        "forecast:GetAccuracyMetrics",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasetImportJobs",
        "forecast:ListDatasets",
        "forecast:ListExplainabilities",
        "forecast:ListExplainabilityExports",
        "forecast:ListForecastExportJobs",
        "forecast:ListForecasts",
        "forecast:ListMonitorEvaluations",
        "forecast:ListMonitors",
        "forecast:ListPredictorBacktestExportJobs",
        "forecast:ListPredictors",
        "forecast:ListWhatIfAnalyses",
        "forecast:ListWhatIfForecastExports",
        "forecast:ListWhatIfForecasts",
        "forecast:QueryForecast",
        "forecast:QueryWhatIfForecast",
        "frauddetector:BatchGetVariable",
        "frauddetector:DescribeDetector",
        "frauddetector:DescribeModelVersions",
        "frauddetector:GetBatchImportJobs",
        "frauddetector:GetBatchPredictionJobs",
        "frauddetector:GetDeleteEventsByEventTypeStatus",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEvent",
```

```
        "frauddetector:GetEventPredictionMetadata",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetKMSEncryptionKey",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModels",
        "frauddetector:GetModelVersion",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListEventPredictions",
        "frauddetector:ListTagsForResource",
        "freertos:Describe*",
        "freertos:List*",
        "freetier:GetAccountActivity",
        "freetier:GetAccountPlanState",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "freetier:ListAccountActivities",
        "fsx:Describe*",
        "fsx:List*",
        "gamelift:Describe*",
        "gamelift:Get*",
        "gamelift:List*",
        "gamelift:ResolveAlias",
        "gamelift:Search*",
        "gameliftstreams:GetApplication",
        "gameliftstreams:GetStreamGroup",
        "gameliftstreams:ListApplications",
        "gameliftstreams:ListStreamGroups",
        "gameliftstreams:ListStreamSessions",
        "gameliftstreams:ListStreamSessionsByAccount",
        "gameliftstreams:ListTagsForResource",
        "gameliftstreams:GetStreamUrl",
        "gameliftstreams:ListApplicationShaderCaches",
        "gameliftstreams:ListStreamUrls",
        "glacier:Describe*",
        "glacier:Get*",
        "glacier:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:BatchGetCrawlers",
```

```
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:BatchGetTriggers",
        "glue:BatchGetWorkflows",
        "glue:CheckSchemaVersionValidity",
        "glue:GetCatalog",
        "glue:GetCatalogImportStatus",
        "glue:GetCatalogs",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlerMetrics",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDataflowGraph",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobBookmark",
        "glue:GetJobRun",
        "glue:GetJobRuns",
        "glue:GetJobs",
        "glue:GetMapping",
        "glue:GetMLTaskRun",
        "glue:GetMLTaskRuns",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetPlan",
        "glue:GetRegistry",
        "glue:GetResourcePolicy",
        "glue:GetSchema",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetSession",
        "glue:GetStatement",
```

```
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetTriggers",
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions",
        "glue:GetWorkflow",
        "glue:GetWorkflowRun",
        "glue:GetWorkflowRunProperties",
        "glue:GetWorkflowRuns",
        "glue:ListCrawlers",
        "glue:ListCrawls",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "glue:ListSchemas",
        "glue:ListSchemaVersions",
        "glue:ListSessions",
        "glue:ListStatements",
        "glue:ListTableOptimizerRuns",
        "glue:ListTriggers",
        "glue:ListWorkflows",
        "glue:QuerySchemaVersionMetadata",
        "glue:SearchTables",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListPermissions",
        "grafana:ListTagsForResource",
        "grafana:ListVersions",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:Get*",
        "greengrass:List*",
        "groundstation:DescribeContactVersion",
        "groundstation:DescribeEphemeris",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMinuteUsage",
```

```
        "groundstation:GetMissionProfile",
        "groundstation:GetSatellite",
        "groundstation:ListAntennas",
        "groundstation:ListConfigs",
        "groundstation:ListContacts",
        "groundstation:ListContactVersions",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListEphemerides",
        "groundstation:ListGroundStationReservations",
        "groundstation:ListGroundStations",
        "groundstation:ListMissionProfiles",
        "groundstation:ListSatellites",
        "groundstation:ListTagsForResource",
        "groundstation:DescribeContact",
        "guardduty:Describe*",
        "guardduty:Get*",
        "guardduty:List*",
        "health:Describe*",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:DescribeFHIRExportJob",
        "healthlake:DescribeFHIRImportJob",
        "healthlake:GetCapabilities",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListFHIRExportJobs",
        "healthlake:ListFHIRImportJobs",
        "healthlake:ListTagsForResource",
        "healthlake:ReadResource",
        "healthlake:SearchWithGet",
        "healthlake:SearchWithPost",
        "iam:Generate*",
        "iam:Get*",
        "iam:List*",
        "iam:Simulate*",
        "identity-sync:GetSyncProfile",
        "identity-sync:GetSyncTarget",
        "identity-sync:ListSyncFilters",
        "identitystore-auth:BatchGetSession",
        "identitystore-auth:ListSessions",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:DescribeUser",
        "identitystore:GetGroupId",
        "identitystore:GetGroupMembershipId",
        "identitystore:GetUserId",
```

```
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "identitystore:ListUsers",
        "imagebuilder:Get*",
        "imagebuilder:List*",
        "importexport:Get*",
        "importexport:List*",
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "inspector2:BatchGetAccountStatus",
        "inspector2:BatchGetCodeSnippet",
        "inspector2:BatchGetFreeTrialInfo",
        "inspector2:BatchGetMemberEc2DeepInspectionStatus",
        "inspector2:DescribeOrganizationConfiguration",
        "inspector2:GetCisScanReport",
        "inspector2:GetConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:GetEc2DeepInspectionConfiguration",
        "inspector2:GetEncryptionKey",
        "inspector2:GetFindingsReportStatus",
        "inspector2:GetMember",
        "inspector2:GetSbomExport",
        "inspector2:ListAccountPermissions",
        "inspector2:ListCisScanConfigurations",
        "inspector2:ListCisScans",
        "inspector2:ListCoverage",
        "inspector2:ListCoverageStatistics",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:ListFilters",
        "inspector2:ListFindingAggregations",
        "inspector2:ListFindings",
        "inspector2:ListMembers",
        "inspector2:ListTagsForResource",
        "inspector2:ListUsageTotals",
        "inspector2:SearchVulnerabilities",
        "inspector2:ListConnectors",
        "internetmonitor:GetHealthEvent",
        "internetmonitor:GetInternetEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListHealthEvents",
```

```
        "internetmonitor:ListInternetEvents",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "interconnect:DescribeConnectionProposal",
        "interconnect:GetConnection",
        "interconnect:GetEnvironment",
        "interconnect:ListAttachPoints",
        "interconnect:ListTagsForResource",
        "interconnect:ListEnvironments",
        "interconnect:ListConnections",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceSummaries",
        "iot:Describe*",
        "iot:Get*",
        "iot:List*",
        "iot1click:DescribeDevice",
        "iot1click:DescribePlacement",
        "iot1click:DescribeProject",
        "iot1click:GetDeviceMethods",
        "iot1click:GetDevicesInPlacement",
        "iot1click:ListDeviceEvents",
        "iot1click:ListDevices",
        "iot1click:ListPlacements",
        "iot1click:ListProjects",
        "iot1click:ListTagsForResource",
        "iotanalytics:Describe*",
        "iotanalytics:Get*",
        "iotanalytics:List*",
        "iotanalytics:SampleChannelData",
        "iotevents:DescribeAlarm",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetector",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:DescribeLoggingOptions",
        "iotevents:ListAlarmModels",
        "iotevents:ListAlarmModelVersions",
        "iotevents:ListAlarms",
        "iotevents:ListDetectorModels",
        "iotevents:ListDetectorModelVersions",
        "iotevents:ListDetectors",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
```

```
        "iotfleethub:DescribeApplication",
        "iotfleethub:ListApplications",
        "iotfleetwise:GetCampaign",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetLoggingOptions",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetRegisterAccountStatus",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:GetVehicleStatus",
        "iotfleetwise:ListCampaigns",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListFleetsForVehicle",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotfleetwise:ListVehiclesInFleet",
        "iotsitewise:Describe*",
        "iotsitewise:Get*",
        "iotsitewise:List*",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetEventConfigurationByResourceTypes",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetLogLevelsByResourceTypes",
        "iotwireless:GetMetricConfiguration",
        "iotwireless:GetMetrics",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetMulticastGroupSession",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetPartnerAccount",
        "iotwireless:GetPosition",
        "iotwireless:GetPositionConfiguration",
        "iotwireless:GetPositionEstimate",
        "iotwireless:GetResourceEventConfiguration",
        "iotwireless:GetResourceLogLevel",
        "iotwireless:GetResourcePosition",
```

```
        "iotwireless:GetServiceEndpoint",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessDeviceImportTask",
        "iotwireless:GetWirelessDeviceStatistics",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayCertificate",
        "iotwireless:GetWirelessGatewayFirmwareInformation",
        "iotwireless:GetWirelessGatewayStatistics",
        "iotwireless:GetWirelessGatewayTask",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListDevicesForWirelessDeviceImportTask",
        "iotwireless:ListEventConfigurations",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListMulticastGroupsByFuotaTask",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListPartnerAccounts",
        "iotwireless:ListPositionConfigurations",
        "iotwireless:ListQueuedMessages",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDeviceImportTasks",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGateways",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:BatchGetChannel",
        "ivs:GetChannel",
        "ivs:GetComposition",
        "ivs:GetEncoderConfiguration",
        "ivs:GetIngestConfiguration",
        "ivs:GetParticipant",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetPublicKey",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStageSession",
        "ivs:GetStorageConfiguration",
        "ivs:GetStream",
        "ivs:GetStreamSession",
        "ivs:ListChannels",
```

```
        "ivs:ListCompositions",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListParticipantEvents",
        "ivs:ListParticipants",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStageSessions",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListStreams",
        "ivs:ListStreamSessions",
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyActionsGroup2",
      "Effect" : "Allow",
      "Action" : [
        "kafka:Describe*",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:Get*",
        "kafka:GetBootstrapBrokers",
        "kafka:GetCompatibleKafkaVersions",
        "kafka:List*",
        "kafka:ListClusterOperations",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurationRevisions",
        "kafka:ListConfigurations",
        "kafka:ListKafkaVersions",
```

```
        "kafka:ListNodes",
        "kafka:ListTagsForResource",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra:BatchGetDocumentStatus",
        "kendra:DescribeDataSource",
        "kendra:DescribeExperience",
        "kendra:DescribeFaq",
        "kendra:DescribeIndex",
        "kendra:DescribePrincipalMapping",
        "kendra:DescribeQuerySuggestionsBlockList",
        "kendra:DescribeQuerySuggestionsConfig",
        "kendra:DescribeThesaurus",
        "kendra:GetQuerySuggestions",
        "kendra:GetSnapshots",
        "kendra:ListDataSources",
        "kendra:ListDataSourceSyncJobs",
        "kendra:ListEntityPersonas",
        "kendra:ListExperienceEntities",
        "kendra:ListExperiences",
        "kendra:ListFaqs",
        "kendra:ListGroupsOlderThanOrderingId",
        "kendra:ListIndices",
        "kendra:ListQuerySuggestionsBlockLists",
        "kendra:ListTagsForResource",
        "kendra:ListThesauri",
        "kendra:Query",
        "kinesis:Describe*",
        "kinesis:Get*",
        "kinesis:List*",
        "kinesisanalytics:Describe*",
        "kinesisanalytics:Discover*",
        "kinesisanalytics:Get*",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kinesisvideo:Get*",
        "kinesisvideo:List*",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
```

```
        "lakeformation:DescribeResource",
        "lakeformation:GetDataCellsFilter",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetEffectivePermissionsForPath",
        "lakeformation:GetLfTag",
        "lakeformation:GetResourceLfTags",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListLfTags",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:ListTableStorageOptimizers",
        "lakeformation:SearchDatabasesByLfTags",
        "lakeformation:SearchTablesByLfTags",
        "lambda:Get*",
        "lambda:List*",
        "launchwizard:DescribeAdditionalNode",
        "launchwizard:DescribeProvisionedApp",
        "launchwizard:DescribeProvisioningEvents",
        "launchwizard:DescribeSettingsSet",
        "launchwizard:GetDeployment",
        "launchwizard:GetInfrastructureSuggestion",
        "launchwizard:GetIpAddress",
        "launchwizard:GetResourceCostEstimate",
        "launchwizard:GetResourceRecommendation",
        "launchwizard:GetSettingsSet",
        "launchwizard:GetWorkload",
        "launchwizard:GetWorkloadAsset",
        "launchwizard:GetWorkloadAssets",
        "launchwizard:GetWorkloadDeploymentPattern",
        "launchwizard:ListAdditionalNodes",
        "launchwizard:ListAllowedResources",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListProvisionedApps",
        "launchwizard:ListResourceCostEstimates",
        "launchwizard:ListSettingsSets",
        "launchwizard:ListTagsForResource",
        "launchwizard:ListWorkloadDeploymentOptions",
        "launchwizard:ListWorkloadDeploymentPatterns",
        "launchwizard:ListWorkloads",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotChannel",
        "lex:DescribeBotLocale",
```

```
        "lex:DescribeBotReplica",
        "lex:DescribeBotVersion",
        "lex:DescribeExport",
        "lex:DescribeImport",
        "lex:DescribeIntent",
        "lex:DescribeResourcePolicy",
        "lex:DescribeSlot",
        "lex:DescribeSlotType",
        "lex:Get*",
        "lex:ListBotAliases",
        "lex:ListBotAliasReplicas",
        "lex:ListBotChannels",
        "lex:ListBotLocales",
        "lex:ListBotReplicas",
        "lex:ListBots",
        "lex:ListBotVersionReplicas",
        "lex:ListBotVersions",
        "lex:ListBuiltInIntents",
        "lex:ListBuiltInSlotTypes",
        "lex:ListExports",
        "lex:ListImports",
        "lex:ListIntents",
        "lex:ListSlots",
        "lex:ListSlotTypes",
        "lex:ListTagsForResource",
        "license-manager:Get*",
        "license-manager:List*",
        "lightsail:GetActiveNames",
        "lightsail:GetAlarms",
        "lightsail:GetAutoSnapshots",
        "lightsail:GetBlueprints",
        "lightsail:GetBucketAccessKeys",
        "lightsail:GetBucketBundles",
        "lightsail:GetBucketMetricData",
        "lightsail:GetBuckets",
        "lightsail:GetBundles",
        "lightsail:GetCertificates",
        "lightsail:GetCloudFormationStackRecords",
        "lightsail:GetContainerAPIMetadata",
        "lightsail:GetContainerImages",
        "lightsail:GetContainerServiceDeployments",
        "lightsail:GetContainerServiceMetricData",
        "lightsail:GetContainerServicePowers",
        "lightsail:GetContainerServices",
```

```
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDistributionBundles",
        "lightsail:GetDistributionLatestCacheReset",
        "lightsail:GetDistributionMetricData",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetExportSnapshotRecords",
        "lightsail:GetInstance",
        "lightsail:GetInstanceMetricData",
        "lightsail:GetInstancePortStates",
        "lightsail:GetInstances",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetInstanceState",
        "lightsail:GetKeyPair",
        "lightsail:GetKeyPairs",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancerMetricData",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetOperation",
        "lightsail:GetOperations",
        "lightsail:GetOperationsForResource",
        "lightsail:GetRegions",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseBlueprints",
        "lightsail:GetRelationalDatabaseBundles",
        "lightsail:GetRelationalDatabaseEvents",
        "lightsail:GetRelationalDatabaseLogEvents",
        "lightsail:GetRelationalDatabaseLogStreams",
        "lightsail:GetRelationalDatabaseMetricData",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "lightsail:Is*",
        "logs:Describe*",
        "logs:FilterLogEvents",
```

```
        "logs:Get*",
        "logs:ListAggregateLogGroupSummaries",
        "logs:ListAnomalies",
        "logs:ListEntitiesForLogGroup",
        "logs:ListIntegrations",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListLogGroupsForEntity",
        "logs:ListLogGroupsForQuery",
        "logs:ListScheduledQueries",
        "logs:ListSourcesForS3TableIntegration",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "logs:StartLiveTail",
        "logs:StartQuery",
        "logs:StopLiveTail",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "lookoutequipment:DescribeDataIngestionJob",
        "lookoutequipment:DescribeDataset",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:DescribeLabel",
        "lookoutequipment:DescribeLabelGroup",
        "lookoutequipment:DescribeModel",
        "lookoutequipment:DescribeModelVersion",
        "lookoutequipment:DescribeResourcePolicy",
        "lookoutequipment:DescribeRetrainingScheduler",
        "lookoutequipment:ListDataIngestionJobs",
        "lookoutequipment:ListDatasets",
        "lookoutequipment:ListInferenceEvents",
        "lookoutequipment:ListInferenceExecutions",
        "lookoutequipment:ListInferenceSchedulers",
        "lookoutequipment:ListLabelGroups",
        "lookoutequipment:ListLabels",
        "lookoutequipment:ListModels",
        "lookoutequipment:ListModelVersions",
        "lookoutequipment:ListRetrainingSchedulers",
        "lookoutequipment:ListSensorStatistics",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:Describe*",
        "lookoutmetrics:Get*",
        "lookoutmetrics:List*",
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
```

```
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModelPackagingJobs",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "m2:GetApplication",
        "m2:GetApplicationVersion",
        "m2:GetBatchJobExecution",
        "m2:GetDataSetDetails",
        "m2:GetDataSetImportTask",
        "m2:GetDeployment",
        "m2:GetEnvironment",
        "m2:ListApplications",
        "m2:ListApplicationVersions",
        "m2:ListBatchJobDefinitions",
        "m2:ListBatchJobExecutions",
        "m2:ListDataSetImportHistory",
        "m2:ListDataSets",
        "m2:ListDeployments",
        "m2:ListEngineVersions",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "machinelearning:Describe*",
        "machinelearning:Get*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:DescribeBuckets",
        "macie2:DescribeClassificationJob",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAdministratorAccount",
        "macie2:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetBucketStatistics",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetClassificationScope",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindings",
        "macie2:GetFindingsFilter",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetFindingStatistics",
        "macie2:GetInvitationsCount",
        "macie2:GetMacieSession",
        "macie2:GetMember",
```

```
        "macie2:GetResourceProfile",
        "macie2:GetRevealConfiguration",
        "macie2:GetSensitiveDataOccurrencesAvailability",
        "macie2:GetSensitivityInspectionTemplate",
        "macie2:GetUsageStatistics",
        "macie2:GetUsageTotals",
        "macie2:ListAllowLists",
        "macie2:ListAutomatedDiscoveryAccounts",
        "macie2:ListClassificationJobs",
        "macie2:ListClassificationScopes",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindings",
        "macie2:ListFindingsFilters",
        "macie2:ListInvitations",
        "macie2:ListMembers",
        "macie2:ListOrganizationAdminAccounts",
        "macie2:ListResourceProfileArtifacts",
        "macie2:ListResourceProfileDetections",
        "macie2:ListSensitivityInspectionTemplates",
        "macie2:ListTagsForResource",
        "macie2:SearchResources",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:GetProposal",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNetworks",
        "managedblockchain:ListNodes",
        "managedblockchain:ListProposals",
        "managedblockchain:ListProposalVotes",
        "managedblockchain:ListTagsForResource",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeFlowSourceMetadata",
        "mediaconnect:DescribeFlowSourceThumbnail",
        "mediaconnect:DescribeGateway",
        "mediaconnect:DescribeGatewayInstance",
        "mediaconnect:DescribeOffering",
        "mediaconnect:DescribeReservation",
        "mediaconnect:DiscoverGatewayPollEndpoint",
        "mediaconnect:GetRouterInput",
        "mediaconnect:GetRouterNetworkInterface",
        "mediaconnect:GetRouterOutput",
        "mediaconnect:ListBridges",
```

```
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGatewayInstances",
        "mediaconnect:ListGateways",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mediaconnect:ListRouterInputs",
        "mediaconnect:ListRouterNetworkInterfaces",
        "mediaconnect:ListRouterOutputs",
        "mediaconnect:ListTagsForResource",
        "mediaconvert:DescribeEndpoints",
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "mediaconvert:Probe",
        "mediaconvert:SearchJobs",
        "medialive:DescribeAccountConfiguration",
        "medialive:DescribeChannel",
        "medialive:DescribeChannelPlacementGroup",
        "medialive:DescribeCluster",
        "medialive:DescribeInput",
        "medialive:DescribeInputDevice",
        "medialive:DescribeInputDeviceThumbnail",
        "medialive:DescribeInputSecurityGroup",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeNetwork",
        "medialive:DescribeOffering",
        "medialive:DescribeReservation",
        "medialive:DescribeSchedule",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:ListChannels",
        "medialive:ListCloudWatchAlarmTemplateGroups",
        "medialive:ListCloudWatchAlarmTemplates",
        "medialive:ListEventBridgeRuleTemplateGroups",
        "medialive:ListEventBridgeRuleTemplates",
        "medialive:ListInputDevices",
        "medialive:ListInputDeviceTransfers",
        "medialive:ListInputs",
        "medialive:ListInputSecurityGroups",
        "medialive:ListMultiplexes",
```

```
        "medialive:ListMultiplexPrograms",
        "medialive:ListOfferings",
        "medialive:ListReservations",
        "medialive:ListSignalMaps",
        "medialive:ListTagsForResource",
        "mediapackage-vod:Describe*",
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetHeadObject",
        "mediapackagev2:GetObject",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediapackagev2:ListTagsForResource",
        "mediastore:DescribeContainer",
        "mediastore:DescribeObject",
        "mediastore:GetContainerPolicy",
        "mediastore:GetCorsPolicy",
        "mediastore:GetLifecyclePolicy",
        "mediastore:GetMetricPolicy",
        "mediastore:GetObject",
        "mediastore:ListContainers",
        "mediastore:ListItems",
        "mediastore:ListTagsForResource",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeEngineVersions",
        "memorydb:DescribeEvents",
        "memorydb:DescribeMultiRegionClusters",
        "memorydb:DescribeMultiRegionParameterGroups",
        "memorydb:DescribeMultiRegionParameters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:DescribeReservedNodes",
        "memorydb:DescribeReservedNodesOfferings",
        "memorydb:DescribeServiceUpdates",
        "memorydb:DescribeSnapshots",
        "memorydb:DescribeSubnetGroups",
```

```
        "memorydb:DescribeUsers",
        "memorydb:ListAllowedMultiRegionClusterUpdates",
        "memorydb:ListAllowedNodeTypeUpdates",
        "memorydb:ListTags",
        "mgh:Describe*",
        "mgh:GetHomeRegion",
        "mgh:List*",
        "mgn:DescribeJobLogItems",
        "mgn:DescribeJobs",
        "mgn:DescribeLaunchConfigurationTemplates",
        "mgn:DescribeReplicationConfigurationTemplates",
        "mgn:DescribeSourceServers",
        "mgn:DescribeVcenterClients",
        "mgn:GetLaunchConfiguration",
        "mgn:GetReplicationConfiguration",
        "mgn:ListApplications",
        "mgn:ListSourceServerActions",
        "mgn:ListTemplateActions",
        "mgn:ListWaves",
        "mobileanalytics:Get*",
        "mobiletargeting:Get*",
        "mobiletargeting:List*",
        "monitron:GetProject",
        "monitron:GetProjectAdminUser",
        "monitron:ListProjects",
        "monitron:ListTagsForResource",
        "mpa:GetApprovalTeam",
        "mpa:GetIdentitySource",
        "mpa:GetPolicyVersion",
        "mpa:GetResourcePolicy",
        "mpa:GetSession",
        "mpa:ListApprovalTeams",
        "mpa:ListIdentitySources",
        "mpa:ListPolicies",
        "mpa:ListPolicyVersions",
        "mpa:ListResourcePolicies",
        "mpa:ListSessions",
        "mpa:ListTagsForResource",
        "mq:Describe*",
        "mq:List*",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeProxy",
```

```
        "network-firewall:DescribeProxyConfiguration",
        "network-firewall:DescribeProxyRule",
        "network-firewall:DescribeProxyRuleGroup",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListProxies",
        "network-firewall:ListProxyConfigurations",
        "network-firewall:ListProxyRuleGroups",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListTLSInspectionConfigurations",
        "networkflowmonitor:GetMonitor",
        "networkflowmonitor:GetScope",
        "networkflowmonitor:ListMonitors",
        "networkflowmonitor:ListScopes",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnections",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetConnectPeerAssociations",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkChangeEvents",
        "networkmanager:GetCoreNetworkChangeSet",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetNetworkResourceCounts",
        "networkmanager:GetNetworkResourceRelationships",
        "networkmanager:GetNetworkResources",
        "networkmanager:GetNetworkRoutes",
        "networkmanager:GetNetworkTelemetry",
        "networkmanager:GetResourcePolicy",
        "networkmanager:GetRouteAnalysis",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayConnectPeerAssociations",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
```

```
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:ListAttachmentRoutingPolicyAssociations",
        "networkmanager:ListAttachments",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListCoreNetworkPolicyVersions",
        "networkmanager:ListCoreNetworkPrefixListAssociations",
        "networkmanager:ListCoreNetworkRoutingInformation",
        "networkmanager:ListCoreNetworks",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "networkmonitor:GetMonitor",
        "networkmonitor:GetProbe",
        "networkmonitor:ListMonitors",
        "networkmonitor:ListTagsForResource",
        "nimble:GetEula",
        "nimble:GetFeatureMap",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileMember",
        "nimble:GetStreamingImage",
        "nimble:GetStreamingSession",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:GetStudioMember",
        "nimble:ListEulaAcceptances",
        "nimble:ListEulas",
        "nimble:ListLaunchProfileMembers",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStreamingSessions",
        "nimble:ListStudioComponents",
        "nimble:ListStudioMembers",
        "nimble:ListStudios",
        "nimble:ListTagsForResource",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:ListTagsForResource",
        "notifications:GetEventRule",
        "notifications:GetFeatureOptInStatus",
        "notifications:GetManagedNotificationChildEvent",
        "notifications:GetManagedNotificationConfiguration",
        "notifications:GetManagedNotificationEvent",
```

```
        "notifications:GetNotificationConfiguration",
        "notifications:GetNotificationEvent",
        "notifications:GetNotificationsAccessForOrganization",
        "notifications:List*",
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListAttachedLinks",
        "oam:ListLinks",
        "oam:ListSinks",
        "observabilityadmin:GetCentralizationRuleForOrganization",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:GetTelemetryEvaluationStatus",
        "observabilityadmin:GetTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:GetTelemetryPipeline",
        "observabilityadmin:GetTelemetryRule",
        "observabilityadmin:GetTelemetryRuleForOrganization",
        "observabilityadmin:ListCentralizationRulesForOrganization",
        "observabilityadmin:ListResourceTelemetry",
        "observabilityadmin:ListResourceTelemetryForOrganization",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:ListTagsForResource",
        "observabilityadmin:ListTelemetryPipelines",
        "observabilityadmin:ListTelemetryRules",
        "observabilityadmin:ListTelemetryRulesForOrganization",
        "observabilityadmin:TestTelemetryPipeline",
        "observabilityadmin:ValidateTelemetryPipelineConfiguration",
        "omics:Get*",
        "omics:List*",
        "one:GetDeviceConfigurationTemplate",
        "one:GetDeviceInstance",
        "one:GetDeviceInstanceConfiguration",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceConfigurationTemplates",
        "one:ListDeviceInstances",
        "one:ListSites",
        "one:ListUsers",
        "opsworks-cm:Describe*",
        "opsworks-cm:List*",
        "opsworks:Describe*",
        "opsworks:Get*",
        "organizations:Describe*",
```

```
        "organizations:List*",
        "osis:GetPipeline",
        "osis:GetPipelineBlueprint",
        "osis:GetPipelineChangeProgress",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "outposts:Get*",
        "outposts:List*",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:GetPublicKeyCertificate",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentInstruments",
        "payments:ListPaymentPreferences",
        "payments:ListPaymentProgramOptions",
        "payments:ListPaymentProgramStatus",
        "payments:ListTagsForResource",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListServicePrincipalNames",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-ad:ListTemplateGroupAccessControlEntries",
        "pca-connector-ad:ListTemplates",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:ListChallengeMetadata",
        "pca-connector-scep:ListConnectors",
        "pca-connector-scep:ListTagsForResource",
        "pcs:GetCluster",
        "pcs:GetComputeNodeGroup",
        "pcs:GetQueue",
        "pcs:ListClusters",
        "pcs:ListComputeNodeGroups",
        "pcs:ListQueues",
```

```
        "pcs:ListTagsForResource",
        "personalize:Describe*",
        "personalize:Get*",
        "personalize:List*",
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "polly:Describe*",
        "polly:Get*",
        "polly:List*",
        "polly:SynthesizeSpeech",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetPriceListFileUrl",
        "pricing:GetProducts",
        "pricing:ListPriceLists",
        "proton:GetDeployment",
        "proton:GetEnvironment",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateVersion",
        "proton:ListDeployments",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplates",
        "proton:ListServiceInstances",
        "proton:ListServices",
        "proton:ListServiceTemplates",
        "proton:ListTagsForResource",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ViewPurchaseOrders",
        "qbusiness:GetApplication",
        "qbusiness:GetChatControlsConfiguration",
```

```
        "qbusiness:GetDataSource",
        "qbusiness:GetGroup",
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetRetriever",
        "qbusiness:GetUser",
        "qbusiness:GetWebExperience",
        "qbusiness:ListApplications",
        "qbusiness:ListDataSources",
        "qbusiness:ListDataSourceSyncJobs",
        "qbusiness:ListGroups",
        "qbusiness:ListIndices",
        "qbusiness:ListPlugins",
        "qbusiness:ListRetrievers",
        "qbusiness:ListSubscriptions",
        "qbusiness:ListTagsForResource",
        "qbusiness:ListWebExperiences",
        "qldb:DescribeJournalKinesisStream",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeLedger",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:ListLedgers",
        "qldb:ListTagsForResource",
        "ram:Get*",
        "ram:List*",
        "rbin:GetRule",
        "rbin:ListRules",
        "rbin:ListTagsForResource",
        "rds:Describe*",
        "rds:Download*",
        "rds:List*",
        "redshift-serverless:GetCustomDomainAssociation",
        "redshift-serverless:GetEndpointAccess",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetRecoveryPoint",
        "redshift-serverless:GetResourcePolicy",
        "redshift-serverless:GetScheduledAction",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetTableRestoreStatus",
```

```
        "redshift-serverless:GetUsageLimit",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListCustomDomainAssociations",
        "redshift-serverless:ListEndpointAccess",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListRecoveryPoints",
        "redshift-serverless:ListScheduledActions",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTableRestoreStatus",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListUsageLimits",
        "redshift-serverless:ListWorkgroups",
        "redshift:Describe*",
        "redshift:GetReservedNodeExchangeOfferings",
        "redshift:ListRecommendations",
        "redshift:View*",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetResourcePolicy",
        "refactor-spaces:GetRoute",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListEnvironmentVpcs",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:CompareFaces",
        "rekognition:DescribeDataset",
        "rekognition:DescribeProjects",
        "rekognition:DescribeProjectVersions",
        "rekognition:DescribeStreamProcessor",
        "rekognition:Detect*",
        "rekognition:GetCelebrityInfo",
        "rekognition:GetCelebrityRecognition",
        "rekognition:GetContentModeration",
        "rekognition:GetFaceDetection",
        "rekognition:GetFaceSearch",
        "rekognition:GetLabelDetection",
        "rekognition:GetPersonTracking",
        "rekognition:GetSegmentDetection",
        "rekognition:GetTextDetection",
        "rekognition:List*",
```

```
        "rekognition:RecognizeCelebrities",
        "rekognition:Search*",
        "resiliencehub:GetFailureModeFinding",
        "resiliencehub:GetPolicy",
        "resiliencehub:GetService",
        "resiliencehub:GetSystem",
        "resiliencehub:GetUserJourney",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppAssessment",
        "resiliencehub:DescribeAppVersion",
        "resiliencehub:DescribeAppVersionAppComponent",
        "resiliencehub:DescribeAppVersionResource",
        "resiliencehub:DescribeAppVersionResourcesResolutionStatus",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeDraftAppVersionResourcesImportStatus",
        "resiliencehub:DescribeMetricsExport",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:DescribeResourceGroupingRecommendationTask",
        "resiliencehub:ListAlarmRecommendations",
        "resiliencehub:ListAppAssessmentComplianceDrifts",
        "resiliencehub:ListAppAssessmentResourceDrifts",
        "resiliencehub:ListAppAssessments",
        "resiliencehub:ListAppComponentCompliances",
        "resiliencehub:ListAppComponentRecommendations",
        "resiliencehub:ListAppInputSources",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionAppComponents",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListAppVersionResources",
        "resiliencehub:ListAppVersions",
        "resiliencehub:ListAssertions",
        "resiliencehub:ListDependencies",
        "resiliencehub:ListFailureModeAssessments",
        "resiliencehub:ListFailureModeFindings",
        "resiliencehub:ListInputSources",
        "resiliencehub:ListMetrics",
        "resiliencehub:ListPolicies",
        "resiliencehub:ListRecommendationTemplates",
        "resiliencehub:ListReports",
        "resiliencehub:ListResources",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListResourceGroupingRecommendations",
        "resiliencehub:ListServices",
        "resiliencehub:ListServiceEvents",
```

```
        "resiliencehub:ListServiceFunctions",
        "resiliencehub:ListServiceEvents",
        "resiliencehub:ListServiceFunctions",
        "resiliencehub:ListServiceTopologyEdges",
        "resiliencehub:ListSopRecommendations",
        "resiliencehub:ListSuggestedResiliencyPolicies",
        "resiliencehub:ListSystems",
        "resiliencehub:ListSystemEvents",
        "resiliencehub:ListTagsForResource",
        "resiliencehub:ListTestRecommendations",
        "resiliencehub:ListUnsupportedAppVersionResources",
        "resiliencehub:ListUserJourneys",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:GetAccountLevelServiceConfiguration",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetManagedView",
        "resource-explorer-2:GetResourceExplorerSetup",
        "resource-explorer-2:GetServiceIndex",
        "resource-explorer-2:GetServiceView",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListIndexesForMembers",
        "resource-explorer-2:ListManagedViews",
        "resource-explorer-2:ListServiceIndexes",
        "resource-explorer-2:ListServiceViews",
        "resource-explorer-2:ListStreamingAccessForServices",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-explorer-2:Search",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*",
        "robomaker:List*",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
```

```
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53-recovery-cluster:Get*",
        "route53-recovery-cluster:ListRoutingControls",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:GetResourcePolicy",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:Get*",
        "route53-recovery-readiness:List*",
        "route53:Get*",
        "route53:List*",
        "route53:Test*",
        "route53domains:Check*",
        "route53domains:Get*",
        "route53domains:List*",
        "route53domains:View*",
        "route53globalresolver:GetAccessSource",
        "route53globalresolver:GetDNSView",
        "route53globalresolver:GetFirewallDomainList",
        "route53globalresolver:GetFirewallRule",
        "route53globalresolver:GetGlobalResolver",
        "route53globalresolver:GetHostedZoneAssociation",
        "route53globalresolver:GetManagedFirewallDomainList",
        "route53globalresolver:ListAccessSources",
        "route53globalresolver:ListAccessTokens",
        "route53globalresolver:ListDNSViews",
        "route53globalresolver:ListFirewallDomainLists",
        "route53globalresolver:ListFirewallDomains",
        "route53globalresolver:ListFirewallRules",
        "route53globalresolver:ListGlobalResolvers",
        "route53globalresolver:ListHostedZoneAssociations",
        "route53globalresolver:ListManagedFirewallDomainLists",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:Get*",
        "route53resolver:List*",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
```

```
        "rum:ListAppMonitors",
        "s3-object-lambda:GetObject",
        "s3-object-lambda:GetObjectAcl",
        "s3-object-lambda:GetObjectLegalHold",
        "s3-object-lambda:GetObjectRetention",
        "s3-object-lambda:GetObjectTagging",
        "s3-object-lambda:GetObjectVersion",
        "s3-object-lambda:GetObjectVersionAcl",
        "s3-object-lambda:GetObjectVersionTagging",
        "s3-object-lambda:ListBucket",
        "s3-object-lambda:ListBucketMultipartUploads",
        "s3-object-lambda:ListBucketVersions",
        "s3-object-lambda:ListMultipartUploadParts",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetBucketVersioning",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:GetObject",
        "s3-outposts:GetObjectTagging",
        "s3-outposts:GetObjectVersion",
        "s3-outposts:GetObjectVersionForReplication",
        "s3-outposts:GetObjectVersionTagging",
        "s3-outposts:GetReplicationConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListBucket",
        "s3-outposts:ListBucketMultipartUploads",
        "s3-outposts:ListBucketVersions",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListMultipartUploadParts",
        "s3-outposts:ListOutpostsWithS3",
        "s3-outposts:ListRegionalBuckets",
        "s3-outposts:ListSharedEndpoints",
        "s3:DescribeJob",
        "s3:Get*",
        "s3:List*",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
        "s3express:GetAccessPointScope",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetLifecycleConfiguration",
```

```
        "s3express:ListAccessPointsForDirectoryBuckets",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:ListTagsForResource",
        "s3files:GetAccessPoint",
        "s3files:GetFileSystem",
        "s3files:GetFileSystemPolicy",
        "s3files:GetMountTarget",
        "s3files:GetSynchronizationConfiguration",
        "s3files:ListAccessPoints",
        "s3files:ListFileSystems",
        "s3files:ListMountTargets",
        "s3files:ListTagsForResource",
        "s3tables:GetNamespace",
        "s3tables:GetTable",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableBucketReplication",
        "s3tables:GetTableBucketStorageClass",
        "s3tables:GetTableData",
        "s3tables:GetTableEncryption",
        "s3tables:GetTableMaintenanceConfiguration",
        "s3tables:GetTableMaintenanceJobStatus",
        "s3tables:GetTableMetadataLocation",
        "s3tables:GetTablePolicy",
        "s3tables:GetTableRecordExpirationConfiguration",
        "s3tables:GetTableRecordExpirationJobStatus",
        "s3tables:GetTableReplication",
        "s3tables:GetTableReplicationStatus",
        "s3tables:GetTableStorageClass",
        "s3tables:ListNamespaces",
        "s3tables:ListTableBuckets",
        "s3tables:ListTables",
        "s3tables:ListTagsForResource",
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:GetVectors",
        "s3vectors:ListIndexes",
        "s3vectors:ListVectorBuckets",
        "s3vectors:ListVectors",
        "s3vectors:QueryVectors",
        "sagemaker:Describe*",
```

```
        "sagemaker:GetSearchSuggestions",
        "sagemaker:List*",
        "sagemaker:Search",
        "savingsplans:DescribeSavingsPlanRates",
        "savingsplans:DescribeSavingsPlans",
        "savingsplans:DescribeSavingsPlansOfferingRates",
        "savingsplans:DescribeSavingsPlansOfferings",
        "savingsplans:ListTagsForResource",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
        "schemas:Describe*",
        "schemas:Get*",
        "schemas:List*",
        "schemas:Search*",
        "sdb:Get*",
        "sdb:List*",
        "sdb:Select*",
        "secretsmanager:Describe*",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:List*",
        "securityagent:BatchGetAgentSpaces",
        "securityagent:BatchGetArtifactMetadata",
        "securityagent:BatchGetCodeReviewJobs",
        "securityagent:BatchGetCodeReviewJobTasks",
        "securityagent:BatchGetCodeReviews",
        "securityagent:BatchGetFindings",
        "securityagent:BatchGetPentestJobContentMetadata",
        "securityagent:BatchGetPentestJobs",
        "securityagent:BatchGetPentestJobTasks",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetTargetDomains",
        "securityagent:GetApplication",
        "securityagent:GetArtifact",
        "securityagent:GetDesignReview",
        "securityagent:GetDesignReviewArtifact",
        "securityagent:GetDesignReviewFeedback",
        "securityagent:GetIntegration",
        "securityagent:ListAgentSpaces",
        "securityagent:ListApplications",
        "securityagent:ListArtifacts",
        "securityagent:ListCodeReviewJobsForCodeReview",
```

```
        "securityagent:ListCodeReviewJobTasks",
        "securityagent:ListCodeReviews",
        "securityagent:ListDesignReviewComments",
        "securityagent:ListDesignReviews",
        "securityagent:ListDiscoveredEndpoints",
        "securityagent:ListSecurityRequirements",
        "securityagent:ListTargetDomains",
        "securityagent:ListFindings",
        "securityagent:ListIntegratedResources",
        "securityagent:ListIntegrations",
        "securityagent:ListMemberships",
        "securityagent:ListPentestJobsForPentest",
        "securityagent:ListPentests",
        "securityagent:ListResourcesFromIntegration",
        "securityagent:ListPentestJobTasks",
        "securityagent:BatchGetValidationRuns",
        "securityagent:GetSecurityRequirementPack",
        "securityagent:ListDiscoveredDomains",
        "securityagent:ListSecurityRequirementPacks",
        "securityhub:BatchGetAutomationRules",
        "securityhub:BatchGetConfigurationPolicyAssociations",
        "securityhub:BatchGetControlEvaluations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:Describe*",
        "securityhub:Get*",
        "securityhub:List*",
        "securitylake:GetDataLakeExceptionSubscription",
        "securitylake:GetDataLakeOrganizationConfiguration",
        "securitylake:GetDataLakeSources",
        "securitylake:GetSubscriber",
        "securitylake:ListDataLakeExceptions",
        "securitylake:ListDataLakes",
        "securitylake:ListLogSources",
        "securitylake:ListSubscribers",
        "securitylake:ListTagsForResource",
        "serverlessrepo:Get*",
        "serverlessrepo:List*",
        "serverlessrepo:SearchApplications",
        "servicecatalog:Describe*",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:List*",
        "servicecatalog:Scan*",
```

```
        "servicecatalog:Search*",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAutoManagementConfiguration",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetQuotaUtilizationReport",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "servicequotas:StartQuotaUtilizationReport",
        "ses:BatchGetMetricData",
        "ses:Describe*",
        "ses:Get*",
        "ses:List*",
        "shield:Describe*",
        "shield:Get*",
        "shield:List*",
        "signer:DescribeSigningJob",
        "signer:GetSigningPlatform",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningJobs",
        "signer:ListSigningPlatforms",
        "signer:ListSigningProfiles",
        "signer:ListTagsForResource",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeAccountLimits",
        "sms-voice:DescribeConfigurationSets",
        "sms-voice:DescribeKeywords",
        "sms-voice:DescribeOptedOutNumbers",
        "sms-voice:DescribeOptOutLists",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeProtectConfigurations",
```

```
        "sms-voice:DescribeRegistrationAttachments",
        "sms-voice:DescribeRegistrationFieldDefinitions",
        "sms-voice:DescribeRegistrationFieldValues",
        "sms-voice:DescribeRegistrations",
        "sms-voice:DescribeRegistrationSectionDefinitions",
        "sms-voice:DescribeRegistrationTypeDefinitions",
        "sms-voice:DescribeRegistrationVersions",
        "sms-voice:DescribeSenderIds",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:DescribeVerifiedDestinationNumbers",
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "snowball:Describe*",
        "snowball:Get*",
        "snowball:List*",
        "sns:Check*",
        "sns:Get*",
        "sns:List*",
        "sqs:Get*",
        "sqs:List*",
        "sqs:Receive*",
        "ssm-contacts:DescribeEngagement",
        "ssm-contacts:DescribePage",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListEngagements",
        "ssm-contacts:ListPageReceipts",
        "ssm-contacts:ListPagesByContact",
        "ssm-contacts:ListPagesByEngagement",
        "ssm-incidents:GetIncidentRecord",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResourcePolicies",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:ListRelatedItems",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-incidents:ListTimelineEvents",
        "ssm-quicksetup:GetConfiguration",
        "ssm-quicksetup:GetConfigurationManager",
```

```
        "ssm-quicksetup:GetServiceSettings",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-quicksetup:ListConfigurations",
        "ssm-quicksetup:ListQuickSetupTypes",
        "ssm-quicksetup:ListTagsForResource",
        "ssm-sap:GetApplication",
        "ssm-sap:GetComponent",
        "ssm-sap:GetConfigurationCheckOperation",
        "ssm-sap:GetDatabase",
        "ssm-sap:GetOperation",
        "ssm-sap:GetResourcePermission",
        "ssm-sap:ListApplications",
        "ssm-sap:ListComponents",
        "ssm-sap:ListConfigurationCheckDefinitions",
        "ssm-sap:ListConfigurationCheckOperations",
        "ssm-sap:ListDatabases",
        "ssm-sap:ListOperationEvents",
        "ssm-sap:ListOperations",
        "ssm-sap:ListSubCheckResults",
        "ssm-sap:ListSubCheckRuleResults",
        "ssm-sap:ListTagsForResource",
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*",
        "sso-directory:Describe*",
        "sso-directory:List*",
        "sso-directory:Search*",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "states:Describe*",
        "states:GetExecutionHistory",
        "states:List*",
        "states:ValidateStateMachineDefinition",
        "storagegateway:Describe*",
        "storagegateway:List*",
        "sts:GetAccessKeyInfo",
        "sts:GetCallerIdentity",
        "sts:GetSessionToken",
        "support:DescribeAttachment",
        "support:DescribeCaseAttributes",
        "support:DescribeCases",
        "support:DescribeCommunication",
        "support:DescribeCommunications",
```

```
        "support:DescribeCreateCaseOptions",
        "support:DescribeIssueTypes",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeSupportedLanguages",
        "support:DescribeSupportLevel",
        "support:DescribeTrustedAdvisorCheckRefreshStatuses",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeTrustedAdvisorChecks",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "support:SearchForCases",
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:ListSupportPlanModifiers",
        "sustainability:GetCarbonFootprintSummary",
        "sustainability:GetEstimatedCarbonEmissions",
        "sustainability:GetEstimatedCarbonEmissionsDimensionValues",
        "sustainability:GetEstimatedWaterAllocation",
        "sustainability:GetEstimatedWaterAllocationDimensionValues",
        "swf:Count*",
        "swf:Describe*",
        "swf:Get*",
        "swf:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "tag:DescribeReportCreation",
        "tag:Get*",
        "tax:GetExemptions",
        "tax:GetTaxInheritance",
        "tax:GetTaxInterview",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
        "timestream:DescribeBatchLoadTask",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListBatchLoadTasks",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "tnb:GetSolFunctionInstance",
```

```
        "tnb:GetSolFunctionPackage",
        "tnb:GetSolFunctionPackageContent",
        "tnb:GetSolFunctionPackageDescriptor",
        "tnb:GetSolNetworkInstance",
        "tnb:GetSolNetworkOperation",
        "tnb:GetSolNetworkPackage",
        "tnb:GetSolNetworkPackageContent",
        "tnb:GetSolNetworkPackageDescriptor",
        "tnb:ListSolFunctionInstances",
        "tnb:ListSolFunctionPackages",
        "tnb:ListSolNetworkInstances",
        "tnb:ListSolNetworkOperations",
        "tnb:ListSolNetworkPackages",
        "tnb:ListTagsForResource",
        "transcribe:Get*",
        "transcribe:List*",
        "transfer:Describe*",
        "transfer:List*",
        "transfer:TestIdentityProvider",
        "transform:GetAccountSettings",
        "transform:GetAgent",
        "transform:GetAgentRuntimeConfiguration",
        "transform:GetConnector",
        "transform:ListAgents",
        "transform:ListConnectors",
        "transform:ListProfiles",
        "transform:ListTagsForResource",
        "transform-custom:GetAnalysis",
        "transform-custom:GetCampaign",
        "transform-custom:GetFinding",
        "transform-custom:GetFindingGroups",
        "transform-custom:GetKnowledgeItem",
        "transform-custom:GetRemediation",
        "transform-custom:GetRepository",
        "transform-custom:GetSource",
        "transform-custom:ListAnalyses",
        "transform-custom:ListCampaigns",
        "transform-custom:ListCampaignRepositories",
        "transform-custom:ListFindings",
        "transform-custom:ListKnowledgeItems",
        "transform-custom:ListRemediations",
        "transform-custom:ListRepositories",
        "transform-custom:ListSources",
        "transform-custom:ListTagsForResource",
```

```
        "transform-custom:ListTransformationPackageMetadata",
        "translate:DescribeTextTranslationJob",
        "translate:GetParallelData",
        "translate:GetTerminology",
        "translate:ListParallelData",
        "translate:ListTerminologies",
        "translate:ListTextTranslationJobs",
        "trustedadvisor:Describe*",
        "trustedadvisor:GetOrganizationRecommendation",
        "trustedadvisor:GetRecommendation",
        "trustedadvisor:ListChecks",
        "trustedadvisor:ListOrganizationRecommendationAccounts",
        "trustedadvisor:ListOrganizationRecommendationResources",
        "trustedadvisor:ListOrganizationRecommendations",
        "trustedadvisor:ListRecommendationResources",
        "trustedadvisor:ListRecommendations",
        "user-subscriptions:ListApplicationClaims",
        "user-subscriptions:ListClaims",
        "user-subscriptions:ListUserSubscriptions",
        "uxc:GetAccountColor",
        "uxc:GetAccountCustomizations",
        "uxc:ListServices",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:IsAuthorized",
        "verifiedpermissions:IsAuthorizedWithToken",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicies",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetAuthPolicy",
        "vpc-lattice:GetDomainVerification",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourceConfiguration",
        "vpc-lattice:GetResourceGateway",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkResourceAssociation",
```

```
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListDomainVerifications",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListResourceConfigurations",
        "vpc-lattice:ListResourceEndpointAssociations",
        "vpc-lattice:ListResourceGateways",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworkResourceAssociations",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListServiceNetworkVpcEndpointAssociations",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "waf-regional:Get*",
        "waf-regional:List*",
        "waf:Get*",
        "waf:List*",
        "wafv2:CheckCapacity",
        "wafv2:Describe*",
        "wafv2:Get*",
        "wafv2:List*",
        "wellarchitected:ExportLens",
        "wellarchitected:GetAnswer",
        "wellarchitected:GetConsolidatedReport",
        "wellarchitected:GetLens",
        "wellarchitected:GetLensReview",
        "wellarchitected:GetLensReviewReport",
        "wellarchitected:GetLensVersionDifference",
        "wellarchitected:GetMilestone",
        "wellarchitected:GetProfile",
        "wellarchitected:GetProfileTemplate",
        "wellarchitected:GetReviewTemplate",
        "wellarchitected:GetReviewTemplateAnswer",
        "wellarchitected:GetReviewTemplateLensReview",
        "wellarchitected:GetWorkload",
        "wellarchitected:List*",
        "workdocs:CheckAlias",
        "workdocs:Describe*",
```

```
        "workdocs:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListUserSettings",
        "workspaces:Describe*",
        "xray:BatchGet*",
        "xray:CancelTraceRetrieval",
        "xray:Get*",
        "xray:ListResourcePolicies",
        "xray:ListRetrievedTraces",
        "xray:ListTagsForResource",
        "xray:StartTraceRetrieval"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ExpressReadOnlySessionObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3express:CreateSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3express:SessionMode" : "ReadOnly"
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ReInventTicketApprovalAccess

Deskripsi: Memberikan peran IAM atau pengguna akses penuh untuk melihat detail biaya re:Invent pass dan menyetujui penagihan ke akun mereka AWS

`ReInventTicketApprovalAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ReInventTicketApprovalAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 Juni 2026, 18:57 UTC
- Waktu teredit: 10 Juni 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/ReInventTicketApprovalAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowBillToAWSActions",
      "Effect" : "Allow",
      "Action" : [
        "eventsbilltoaws:info",
        "eventsbilltoaws:approve"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ResourceGroupsandTagEditorFullAccess

Deskripsi: Menyediakan akses penuh ke Grup Sumber Daya dan Editor Tag.

`ResourceGroupsandTagEditorFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ResourceGroupsandTagEditorFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC

- Waktu teredit: 10 Agustus 2023, 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "tag:TagResources",
        "tag:UntagResources",
        "resource-groups:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ResourceGroupsandTagEditorReadOnlyAccess

Deskripsi: Menyediakan akses untuk menggunakan Grup Sumber Daya dan Editor Tag, tetapi tidak mengizinkan pengeditan tag melalui Editor Tag.

`ResourceGroupsandTagEditorReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ResourceGroupsandTagEditorReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu teredit: 10 Agustus 2023, 13:42 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:getResources",
```

```
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ResourceGroupsServiceRolePolicy

Deskripsi: Men AWS gizinkan Grup Sumber Daya untuk men AWS anyakan layanan yang memiliki sumber daya Anda agar grup tetap mutakhir

`ResourceGroupsServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 05 Januari 2023, 16:57 UTC
- Waktu teredit: 05 Januari 2023, 16:57 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/ResourceGroupsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ResourceGroupsTaggingAPITagUntagSupportedResources

Deskripsi: Memberikan izin untuk menandai dan menghapus tag semua sumber daya yang didukung oleh API Penandaan Grup Sumber Daya. Kebijakan ini juga memberikan izin yang diperlukan untuk mengambil semua sumber daya yang ditandai, atau diberi tag sebelumnya, melalui API Penandaan Grup Sumber Daya.

`ResourceGroupsTaggingAPITagUntagSupportedResources`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ResourceGroupsTaggingAPITagUntagSupportedResources` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Oktober 2024, 11:11 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsTaggingAPITagUntagSupportedResources`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:TagResource",
        "a4b:UntagResource",
        "access-analyzer:TagResource",
        "access-analyzer:UntagResource",
        "acm-pca:TagCertificateAuthority",
        "acm-pca:UntagCertificateAuthority",
        "acm:AddTagsToCertificate",
        "acm:RemoveTagsFromCertificate",
```

```
        "amplify:TagResource",
        "amplify:UntagResource",
        "appconfig:TagResource",
        "appconfig:UntagResource",
        "appflow:TagResource",
        "appflow:UntagResource",
        "appmesh:TagResource",
        "appmesh:UntagResource",
        "appstream:TagResource",
        "appstream:UntagResource",
        "appsync:TagResource",
        "appsync:UntagResource",
        "athena:TagResource",
        "athena:UntagResource",
        "auditmanager:TagResource",
        "auditmanager:UntagResource",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteTags",
        "backup:TagResource",
        "backup:UntagResource",
        "batch:TagResource",
        "batch:UntagResource",
        "braket:TagResource",
        "braket:UntagResource",
        "cassandra:TagResource",
        "cassandra:UntagResource",
        "chime:TagResource",
        "chime:UntagResource",
        "cloud9:TagResource",
        "cloud9:UntagResource",
        "clouddirectory:TagResource",
        "clouddirectory:UntagResource",
        "cloudfront:TagResource",
        "cloudfront:UntagResource",
        "cloudhsm:TagResource",
        "cloudhsm:UntagResource",
        "cloudtrail:AddTags",
        "cloudtrail:RemoveTags",
        "cloudwatch:TagResource",
        "cloudwatch:UntagResource",
        "codeartifact:TagResource",
        "codeartifact:UntagResource",
        "codecommit:TagResource",
        "codecommit:UntagResource",
```

```
        "codedeploy:AddTagsToOnPremisesInstances",
        "codedeploy:RemoveTagsFromOnPremisesInstances",
        "codedeploy:TagResource",
        "codedeploy:UntagResource",
        "codeguru-profiler:TagResource",
        "codeguru-profiler:UntagResource",
        "codepipeline:TagResource",
        "codepipeline:UntagResource",
        "codestar-connections:TagResource",
        "codestar-connections:UntagResource",
        "codestar:TagProject",
        "codestar:UntagProject",
        "cognito-identity:TagResource",
        "cognito-identity:UntagResource",
        "cognito-idp:TagResource",
        "cognito-idp:UntagResource",
        "comprehend:TagResource",
        "comprehend:UntagResource",
        "config:TagResource",
        "config:UntagResource",
        "connect:TagResource",
        "connect:UntagResource",
        "dataexchange:TagResource",
        "dataexchange:UntagResource",
        "datapipeline:AddTags",
        "datapipeline:RemoveTags",
        "datasync:TagResource",
        "datasync:UntagResource",
        "deepcomposer:TagResource",
        "deepcomposer:UntagResource",
        "detective:TagResource",
        "detective:UntagResource",
        "devicefarm:TagResource",
        "devicefarm:UntagResource",
        "directconnect:TagResource",
        "directconnect:UntagResource",
        "dlm:TagResource",
        "dlm:UntagResource",
        "dms:AddTagsToResource",
        "dms:RemoveTagsFromResource",
        "dynamodb:TagResource",
        "dynamodb:UntagResource",
        "ec2:CreateTags",
        "ec2:DeleteTags",
```

```
        "ecr:TagResource",
        "ecr:UntagResource",
        "ecs:TagResource",
        "ecs:UntagResource",
        "eks:TagResource",
        "eks:UntagResource",
        "elastic-inference:TagResource",
        "elastic-inference:UntagResource",
        "elasticache:AddTagsToResource",
        "elasticache:RemoveTagsFromResource",
        "elasticbeanstalk:UpdateTagsForResource",
        "elasticfilesystem:CreateTags",
        "elasticfilesystem:DeleteTags",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:RemoveTags",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:RemoveTags",
        "emr-containers:TagResource",
        "emr-containers:UntagResource",
        "es:AddTags",
        "es:RemoveTags",
        "events:TagResource",
        "events:UntagResource",
        "firehose:TagDeliveryStream",
        "firehose:UntagDeliveryStream",
        "fms:TagResource",
        "fms:UntagResource",
        "forecast:TagResource",
        "forecast:UntagResource",
        "frauddetector:TagResource",
        "frauddetector:UntagResource",
        "fsx:TagResource",
        "fsx:UntagResource",
        "gamelift:TagResource",
        "gamelift:UntagResource",
        "glacier:AddTagsToVault",
        "glacier:RemoveTagsFromVault",
        "globalaccelerator:TagResource",
        "globalaccelerator:UntagResource",
        "glue:TagResource",
        "glue:UntagResource",
        "greengrass:TagResource",
        "greengrass:UntagResource",
        "groundstation:TagResource",
```

```
        "groundstation:UntagResource",
        "guardduty:TagResource",
        "guardduty:UntagResource",
        "iam:TagInstanceProfile",
        "iam:TagMFADevice",
        "iam:TagOpenIDConnectProvider",
        "iam:TagPolicy",
        "iam:TagRole",
        "iam:TagSAMLProvider",
        "iam:TagServerCertificate",
        "iam:TagUser",
        "iam:UntagInstanceProfile",
        "iam:UntagMFADevice",
        "iam:UntagOpenIDConnectProvider",
        "iam:UntagPolicy",
        "iam:UntagRole",
        "iam:UntagSAMLProvider",
        "iam:UntagServerCertificate",
        "iam:UntagUser",
        "imagebuilder:TagResource",
        "imagebuilder:UntagResource",
        "inspector:ListTagsForResource",
        "inspector:SetTagsForResource",
        "iot1click:TagResource",
        "iot1click:UntagResource",
        "iot:TagResource",
        "iot:UntagResource",
        "iotanalytics:TagResource",
        "iotanalytics:UntagResource",
        "iotdeviceadvisor:TagResource",
        "iotdeviceadvisor:UntagResource",
        "iotevents:TagResource",
        "iotevents:UntagResource",
        "iotfleethub:TagResource",
        "iotfleethub:UntagResource",
        "iotsitewise:TagResource",
        "iotsitewise:UntagResource",
        "iottwinmaker:TagResource",
        "iottwinmaker:UntagResource",
        "iotwireless:TagResource",
        "iotwireless:UntagResource",
        "ivs:TagResource",
        "ivs:UntagResource",
        "kafka:TagResource",
```

```
        "kafka:UntagResource",
        "kendra:TagResource",
        "kendra:UntagResource",
        "kinesis:AddTagsToStream",
        "kinesis:RemoveTagsFromStream",
        "kinesisanalytics:TagResource",
        "kinesisanalytics:UntagResource",
        "kms:TagResource",
        "kms:UntagResource",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lex:TagResource",
        "lex:UntagResource",
        "license-manager:TagResource",
        "license-manager:UntagResource",
        "lightsail:TagResource",
        "lightsail:UntagResource",
        "logs:TagLogGroup",
        "logs:TagResource",
        "logs:UntagLogGroup",
        "logs:UntagResource",
        "lookoutequipment:TagResource",
        "lookoutequipment:UntagResource",
        "machinelearning:AddTags",
        "machinelearning:DeleteTags",
        "macie2:TagResource",
        "macie2:UntagResource",
        "managedblockchain:TagResource",
        "managedblockchain:UntagResource",
        "mediaconnect:TagResource",
        "mediaconnect:UntagResource",
        "mediaconvert:TagResource",
        "mediaconvert:UntagResource",
        "medialive:CreateTags",
        "medialive:DeleteTags",
        "mediapackage-vod:TagResource",
        "mediapackage-vod:UntagResource",
        "mediapackage:TagResource",
        "mediapackage:UntagResource",
        "mediatailor:TagResource",
        "mediatailor:UntagResource",
        "mobiletargeting:TagResource",
        "mobiletargeting:UntagResource",
        "mq:CreateTags",
```

```
        "mq:DeleteTags",
        "neptune-graph:TagResource",
        "neptune-graph:UntagResource",
        "network-firewall:TagResource",
        "network-firewall:UntagResource",
        "networkmanager:TagResource",
        "networkmanager:UntagResource",
        "opsworks-cm:TagResource",
        "opsworks-cm:UntagResource",
        "opsworks:TagResource",
        "opsworks:UntagResource",
        "organizations:TagResource",
        "organizations:UntagResource",
        "outposts:TagResource",
        "outposts:UntagResource",
        "qldb:TagResource",
        "qldb:UntagResource",
        "quicksight:TagResource",
        "quicksight:UntagResource",
        "ram:TagResource",
        "ram:UntagResource",
        "rds:AddTagsToResource",
        "rds:RemoveTagsFromResource",
        "redshift:CreateTags",
        "redshift:DeleteTags",
        "resource-explorer-2:TagResource",
        "resource-explorer-2:UntagResource",
        "resource-groups:Tag",
        "resource-groups:Untag",
        "robomaker:TagResource",
        "robomaker:UntagResource",
        "route53:ChangeTagsForResource",
        "route53domains:DeleteTagsForDomain",
        "route53domains:UpdateTagsForDomain",
        "route53resolver:TagResource",
        "route53resolver:UntagResource",
        "s3:GetBucketTagging",
        "s3:GetJobTagging",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionTagging",
        "s3:GetStorageLensConfigurationTagging",
        "s3:DeleteJobTagging",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersionTagging",
```

```
        "s3:PutBucketTagging",
        "s3:PutJobTagging",
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging",
        "s3:PutStorageLensConfigurationTagging",
        "s3:DeleteStorageLensConfigurationTagging",
        "s3:TagResource",
        "s3:UntagResource",
        "sagemaker:AddTags",
        "sagemaker:DeleteTags",
        "savingsplans:TagResource",
        "savingsplans:UntagResource",
        "schemas:TagResource",
        "schemas:UntagResource",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource",
        "securityhub:TagResource",
        "securityhub:UntagResource",
        "servicediscovery:TagResource",
        "servicediscovery:UntagResource",
        "servicequotas:TagResource",
        "servicequotas:UntagResource",
        "ses:TagResource",
        "ses:UntagResource",
        "sns:TagResource",
        "sns:UntagResource",
        "sqs:TagQueue",
        "sqs:UntagQueue",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "states:TagResource",
        "states:UntagResource",
        "storagegateway:AddTagsToResource",
        "storagegateway:RemoveTagsFromResource",
        "swf:TagResource",
        "swf:UntagResource",
        "synthetics:TagResource",
        "synthetics:UntagResource",
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "transfer:TagResource",
        "transfer:UntagResource",
        "waf-regional:TagResource",
```

```
        "waf-regional:UntagResource",
        "waf:TagResource",
        "waf:UntagResource",
        "wafv2:TagResource",
        "wafv2:UntagResource",
        "worklink:TagResource",
        "worklink:UntagResource",
        "workmail:TagResource",
        "workmail:UntagResource",
        "workspaces:CreateTags",
        "workspaces:DeleteTags",
        "xray:TagResource",
        "xray:UntagResource",
        "kinesisvideo:TagResource",
        "kinesisvideo:UntagResource",
        "redshift-serverless:TagResource",
        "redshift-serverless:UntagResource",
        "route53-recovery-control-config:TagResource",
        "route53-recovery-control-config:UntagResource",
        "route53-recovery-readiness:TagResource",
        "route53-recovery-readiness:UntagResource",
        "ssm-contacts:TagResource",
        "ssm-contacts:UntagResource",
        "ssm-incidents:TagResource",
        "ssm-incidents:UntagResource",
        "vpc-lattice:TagResource",
        "vpc-lattice:UntagResource",
        "workspaces-web:TagResource",
        "workspaces-web:UntagResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ROSAAmazonEBSCSIDriverOperatorPolicy

Deskripsi: Mengiz OpenShift inkan Operator Driver Antarmuka Penyimpanan Kontainer (CSI) Amazon EBS untuk menginstal dan memelihara driver Amazon EBS CSI pada cluster Red Hat OpenShift Service on AWS (ROSA). Driver Amazon EBS CSI memungkinkan klaster ROSA mengelola siklus hidup volume Amazon EBS untuk volume persisten.

`ROSAAmazonEBSCSIDriverOperatorPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAAmazonEBSCSIDriverOperatorPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 April 2023, 22:36 UTC
- Waktu teredit: 19 Agustus 2026, 05:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAAmazonEBSCSIDriverOperatorPolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyDescribeOperations",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVolumeStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateAndCopyVolumesWithManagedTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CopyManagedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/vol-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CopyUserBroughtVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyVolumes"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:volume/vol-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsWithManagedTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsFromManagedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsFromUserBroughtVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "ManageManagedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolume",
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ManageUserBroughtVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolume",
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "CreateVolumesFromAndEnableFSROnManagedSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateVolumesFromAndEnableFSROnUserBroughtSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "AttachDetachVolumesToManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteAndLockManagedSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:LockSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "DeleteAndLockUserBroughtSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:LockSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "TagResourcesOnCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot",
            "CopyVolumes"
          ]
        }
      }
    },
    {
      "Sid" : "ModifyTagsOnManagedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringNotEquals" : {
          "aws:TagKeys" : [
            "red-hat-managed",
            "ebs.csi.aws.com/cluster",
            "kubernetes.io/created-for/pvc/name"
          ]
        }
      }
    },
    {
      "Sid" : "ModifyTagsOnUserBroughtVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringNotEquals" : {
          "aws:TagKeys" : [
            "red-hat-managed",
            "red-hat",
            "ebs.csi.aws.com/cluster",
            "kubernetes.io/created-for/pvc/name"
          ]
        }
      }
    },
    {
      "Sid" : "KMSEncryptedVolumes",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : false
        },
        "ForAllValues:StringEquals" : {
          "kms:EncryptionContextKeys" : [
            "aws:ebs:id"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "StringEquals" : {
          "kms:GrantConstraintType" : "EncryptionContextSubset",
          "aws:ResourceTag/red-hat" : "true"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : false
```

```
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo"
          ],
          "kms:EncryptionContextKeys" : [
            "aws:ebs:id"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeKMSKeysForEBSVolumeEncryption",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ROSACloudNetworkConfigOperatorPolicy

Deskripsi: Mengiz OpenShift inkan Operator Pengontrol Konfigurasi Jaringan Cloud menyediakan dan mengelola sumber daya jaringan untuk digunakan oleh hamparan jaringan cluster Red Hat OpenShift Service on AWS (ROSA). Operator Jaringan OpenShift Cloud berinteraksi dengan AWS API atas nama plugin jaringan melalui CustomResourceDefinitions. Operator menggunakan izin kebijakan ini untuk mengelola alamat IP pribadi untuk instans Amazon EC2 sebagai bagian dari klaster ROSA.

`ROSACloudNetworkConfigOperatorPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSACloudNetworkConfigOperatorPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 April 2023, 22:34 UTC
- Waktu teredit: 20 April 2023, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkResources",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModifyEIPs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnassignPrivateIpAddresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ROSAControlPlaneOperatorPolicy

Deskripsi: Mengizinkan Red Hat OpenShift Service pada pesawat kontrol AWS (ROSA) untuk mengelola sumber daya cluster ROSA Amazon EC2 dan Amazon Route 53.

`ROSAControlPlaneOperatorPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAControlPlaneOperatorPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 24 April 2023, 23:02 UTC
- Waktu teredit: 28 Juli 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "route53:ListHostedZones"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CreateSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupIngressEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupsVPCNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "ListResourceRecordSets",
      "Effect" : "Allow",
      "Action" : [
        "route53:ListResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ChangeResourceRecordSetsRestrictedRecordNames",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.hypershift.local"
          ]
        }
      }
    },
    {
      "Sid" : "VPCEndpointWithCondition",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointResourceTagCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "ManageVPCEndpointWithCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyVPCEndpointNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "CreateTagsRestrictedActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpcEndpoint",
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "AddDeleteTagsRedHatManagedSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        },
        "ForAllValues:StringNotEquals" : {
          "aws:TagKeys" : [
            "red-hat-managed"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ROSAImageRegistryOperatorPolicy

Deskripsi: Men OpenShift gizinkan Operator Registri Gambar menyediakan dan mengelola bucket dan objek Amazon S3 untuk digunakan oleh Red Hat OpenShift Service on AWS (ROSA) in-cluster image registry untuk memenuhi persyaratan penyimpanan ROSA. Operator Registri OpenShift Gambar menginstal dan memelihara registri internal OpenShift cluster Red Hat.

`ROSAImageRegistryOperatorPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAImageRegistryOperatorPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 27 April 2023, 20:13 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAImageRegistryOperatorPolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSpecificBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
```

```
        "s3:DeleteBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetBucketLocation",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}?",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}"
      ]
    },
    {
      "Sid" : "AllowSpecificObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*/*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}?/*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ROSAIngressOperatorPolicy

Deskripsi: Mengiz OpenShift inkan Operator Ingress untuk menyediakan dan mengelola penyeimbang beban dan konfigurasi sistem nama domain (DNS) untuk Red Hat OpenShift Service pada klaster AWS (ROSA). Kebijakan ini memungkinkan akses baca ke nilai tag, yang difilter operator untuk sumber daya Route 53 untuk menemukan zona yang dihosting.

`ROSAIngressOperatorPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAIngressOperatorPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 April 2023, 22:37 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "route53:ListHostedZones",
        "tag:GetResources"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.openshiftapps.com",
            "*.devshift.org",
            "*.openshiftusgov.com",
            "*.devshiftusgov.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ROSAInstallerPolicy

Deskripsi: Mengizinkan penginstal Red Hat OpenShift Service on AWS (ROSA) untuk mengelola AWS sumber daya yang mendukung instalasi klaster ROSA. Ini termasuk mengelola profil instance untuk node pekerja ROSA.

`ROSAInstallerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAInstallerPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Juni 2023, 21:00 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeCapacityReservations",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeLoadBalancers",
```

```
        "iam:GetOpenIDConnectProvider",
        "iam:GetRole",
        "route53:GetHostedZone",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53:GetAccountLimit",
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToEC2",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/*-ROSA-Worker-Role"
      ],
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ]
    },
    {
      "Sid" : "CreateInstanceProfiles",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:TagInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "GetSecretValue",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "Route53ManageRecords",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.openshiftapps.com",
            "*.devshift.org",
            "*.hypershift.local",
            "*.openshiftusgov.com",
            "*.devshiftusgov.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "Route53Manage",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeTagsForResource",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "RunInstancesNoCondition",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RunInstancesRestrictedRequestTag",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesRedHatOwnedAMIs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : [
            "531415883065",
            "251351625822",
            "210686502322"
          ]
        }
      }
    },
    {
      "Sid" : "ManageInstancesRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:GetConsoleOutput"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "CreateGrantRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Sid" : "ManagedKMSRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupIngressEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupsVPCNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "CreateTagsRestrictedActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsK8sSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "DeleteTagsK8sSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "ListPoliciesAttachedToRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ROSAKarpenterControllerPolicy

Deskripsi: Memberikan izin bagi pengontrol ROSA Karpenter untuk menyediakan dan mengelola instans EC2 secara dinamis untuk Red Hat OpenShift Service pada klaster bidang kontrol yang dihosting AWS (ROSA). Ini termasuk manajemen siklus hidup armada dan instans EC2, kueri harga instans, operasi KMS untuk enkripsi volume EBS dengan kunci yang dikelola pelanggan, dan manajemen profil instans IAM.

`ROSAKarpenterControllerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAKarpenterControllerPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 27 Juli 2026, 16:42 UTC
- Waktu teredit: 27 Juli 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKarpenterControllerPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PricingReadActions",
      "Effect" : "Allow",
      "Action" : [
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeKMSKeysForEBSVolumeEncryption",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CryptoOpsForEBSVolumeEncryption",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
```

```
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "kms:EncryptionContextKeys" : [
            "aws:ebs:id"
          ]
        }
      }
    },
    {
      "Sid" : "CreateGrantForEBSVolumeEncryption",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "StringEquals" : {
          "kms:GrantConstraintType" : "EncryptionContextSubset"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo"
          ],
          "kms:EncryptionContextKeys" : [
            "aws:ebs:id"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "CreateEC2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ]
    },
    {
      "Sid" : "CreateEC2ResourcesWithApprovedAMIs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : [
            "531415883065",
            "251351625822",
            "210686502322"
          ]
        }
      }
    },
    {
      "Sid" : "CreateEC2ResourcesWithTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
```

```
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:spot-instances-request/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEC2ResourcesLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:spot-instances-request/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateFleet",
            "CreateLaunchTemplate"
```

```
        ],
        "aws:RequestTag/red-hat-managed" : "true"
      }
    }
  },
  {
    "Sid" : "ManageTagsOnManagedResources",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat-managed" : "true"
      }
    }
  },
  {
    "Sid" : "TerminateManagedResources",
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances",
      "ec2:DeleteLaunchTemplate"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:launch-template/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat-managed" : "true"
      }
    }
  },
  {
    "Sid" : "PassInstanceRole",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "arn:aws:iam::*:role/*-ROSA-Worker-Role",
    "Condition" : {
      "StringEquals" : {
```

```
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ]
    },
    {
      "Sid" : "CreateInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:TagInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ReadInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfiles"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ROSAKMSProviderPolicy

Deskripsi: Mengizinkan Penyedia AWS Enkripsi ROSA bawaan untuk mengelola AWS kunci Key Management Service (KMS) untuk mendukung enkripsi data etcd menggunakan kunci AWS KMS yang disediakan pelanggan. Kebijakan ini memungkinkan enkripsi dan dekripsi data menggunakan kunci KMS.

`ROSAKMSProviderPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAKMSProviderPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 27 April 2023, 20:10 UTC
- Waktu teredit: 27 April 2023, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKMSProviderPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VolumeEncryption",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ROSAKubeControllerPolicy

Deskripsi: Mengizinkan pengontrol ROSA Kubernetes mengelola sumber daya Amazon EC2, Elastic Load Balancing (ELB), dan AWS Key Management Service (KMS) untuk cluster ROSA.

`ROSAKubeControllerPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAKubeControllerPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 27 April 2023, 20:09 UTC
- Waktu teredit: 17 September 2026, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeLoadBalancerPolicies"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "LoadBalanacerManagement",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateLoadBalancerPolicy",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateTargetGroup",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "LoadBalanacerManagementResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:SetSecurityGroups",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:DeleteLoadBalancerListeners",
        "elasticloadbalancing:AttachLoadBalancerToSubnets",
        "elasticloadbalancing:DetachLoadBalancerFromSubnets",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateListeners",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true",
          "aws:ResourceTag/red-hat-managed" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "CreateLoadBalancer",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "ModifySecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid" : "ManageTargetGroup",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:ModifyTargetGroupAttributes",
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ROSAManageSubscription

Deskripsi: Kebijakan ini memberikan izin yang diperlukan untuk mengelola langganan OpenShift Layanan Red Hat pada AWS (ROSA).

`ROSAManageSubscription`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAManageSubscription` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 April 2022, 20:58 UTC
- Waktu teredit: 04 Agustus 2023, 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/ROSAManageSubscription`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "34850061-abaf-402d-92df-94325c9e947f",
            "bfdca560-2c78-4e64-8193-794c159e6d30"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ROSANodePoolManagementPolicy

Deskripsi: Mengizinkan Red Hat OpenShift Service on AWS (ROSA) mengelola instans cluster EC2 sebagai node pekerja, termasuk izin untuk mengonfigurasi grup keamanan dan tag instance dan volume. Kebijakan ini juga memungkinkan penggunaan instans EC2 dengan enkripsi disk yang disediakan oleh AWS kunci Key Management Service (KMS).

`ROSANodePoolManagementPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSANodePoolManagementPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 08 Juni 2023, 20:48 UTC
- Waktu teredit: 29 Juli 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
```

```
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:*:iam::*:role/aws-service-role/elasticloadbalancing.amazonaws.com/
AWSServiceRoleForElasticLoadBalancing"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassWorkerRole",
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:*:iam::*:role/*-ROSA-Worker-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AuthorizeSecurityGroupIngressRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkInterfacesNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
```

```
    },
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileVolume",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesRequest",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ]
    },
    {
      "Sid" : "RunInstancesRedHatAMI",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : [
            "531415883065",
            "251351625822"
          ]
        }
      }
    },
    {
      "Sid" : "NodePoolSQSActions",
      "Effect" : "Allow",
      "Action" : [
        "sqs:DeleteMessage",
```

```
        "sqs:ReceiveMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "ManagedKMSRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "CreateGrantRestricted",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ROSASharedVPCEndpointPolicy

Deskripsi: Mengizinkan penginstal Red Hat OpenShift Service on AWS (ROSA) untuk mengkonfigurasi Titik Akhir VPC dan Grup Keamanan. Ditujukan untuk digunakan pada VPC bersama.

`ROSASharedVPCEndpointPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSASharedVPCEndpointPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Agustus 2025, 17:19 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/ROSASharedVPCEndpointPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "SecurityGroupIngressEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupsVPCNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "VPCEndpointWithCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "VPCEndpointResourceTagCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "ManageVPCEndpointWithCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "ModifyVPCEndpoingNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "CreateTagsRestrictedActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpcEndpoint",
            "CreateSecurityGroup"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ROSASharedVPCRoute53Policy

Deskripsi: Mengizinkan penginstal Red Hat OpenShift Service on AWS (ROSA) untuk mengkonfigurasi catatan Route53. Ditujukan untuk digunakan pada VPC bersama.

`ROSASharedVPCRoute53Policy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSASharedVPCRoute53Policy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Agustus 2025, 17:19 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/ROSASharedVPCRoute53Policy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListResourceRecordSets",
        "route53:ListHostedZones",
```

```
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ChangeResourceRecordSetsRestrictedRecordNames",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.hypershift.local",
            "*.openshiftapps.com",
            "*.devshift.org",
            "*.openshiftusgov.com",
            "*.devshiftusgov.com"
          ]
        }
      }
    },
    {
      "Sid" : "ChangeTagsForResourceNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ROSASRESupportPolicy

Deskripsi: Menyediakan rekayasa keandalan situs ROSA (SRE) izin yang diperlukan untuk mengamati, mendiagnosis, dan mendukung AWS sumber daya yang terkait dengan Red Hat OpenShift Service on AWS (ROSA) cluster, termasuk kemampuan untuk mengubah status node cluster ROSA.

`ROSASRESupportPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSASRESupportPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Juni 2023, 14:36 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions",
        "sts:DecodeAuthorizationMessage"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Route53",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:GetHostedZoneCount",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DecribeIAMRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2DescribeInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeScheduledInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "VPCNetwork",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Cloudtrail",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Cloudwatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVolumeStatus"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "DescribeLoadBalancers",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeSSLPolicies",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeAddressesAttribute",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeAddressesAttribute",
      "Resource" : "arn:aws:ec2:*:*:elastic-ip/*"
    },
    {
      "Sid" : "DescribeInstance",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeSpotFleetInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSpotFleetInstances",
      "Resource" : "arn:aws:ec2:*:*:spot-fleet-request/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeVolumeAttribute",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeVolumeAttribute",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "ManageInstanceLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ROSAWorkerInstancePolicy

Deskripsi: Mengizinkan Red Hat OpenShift Service pada node pekerja AWS (ROSA) di akses baca-saja akun Anda ke instans Amazon EC2 dan Wilayah AWS untuk manajemen siklus hidup simpul komputasi.

`ROSAWorkerInstancePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAWorkerInstancePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 April 2023, 22:35 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2DescribeInstancesRegions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECRGetAuthorizationToken",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECRReadOnlyAccessRedHatManaged",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

Route53RecoveryReadinessServiceRolePolicy

Deskripsi: Kebijakan Peran Terkait Layanan untuk Kesiapan Pemulihan Route 53

`Route53RecoveryReadinessServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 15 Juli 2021, 16:06 UTC
- Waktu teredit: 14 Februari 2023, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/servicequotas.amazonaws.com/
AWSServiceRoleForServiceQuotas",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "servicequotas.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:ListProvisionedConcurrencyConfigs",
        "lambda:ListAliases",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBClusters"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "arn:aws:rds:*:*:db:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ListResourceRecordSets"
      ],
      "Resource" : "arn:aws:route53:::hostedzone/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHealthCheck",
        "route53:GetHealthCheckStatus"
      ],
      "Resource" : "arn:aws:route53:::healthcheck/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:RequestServiceQuotaIncrease"
      ],
      "Resource" : "arn:aws:servicequotas:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl"
      ],
      "Resource" : "arn:aws:sqs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeLoadBalancerTargetGroups",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribePolicies",
```

```
        "cloudwatch:GetMetricData",
        "cloudwatch:DescribeAlarms",
        "dynamodb:DescribeLimits",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "kafka:DescribeCluster",
        "kafka:DescribeConfigurationRevision",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "rds:DescribeAccountAttributes",
        "route53:GetHostedZone",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "sns:GetEndpointAttributes",
        "sns:GetSubscriptionAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

Route53ResolverServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Route53 Resolver

`Route53ResolverServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 12 Agustus 2020, 17:47 UTC
- Waktu teredit: 12 Agustus 2020, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
```

```
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "s3:GetBucketPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

RTBFabricServiceRolePolicy

Deskripsi: Peran terkait layanan yang diperlukan untuk AWS RTBFabric untuk membuat dan mengelola sumber daya antarmuka jaringan Anda dan memberikan metrik.

`RTBFabricServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 16 Oktober 2025, 16:49 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/RTBFabricServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RTBFabricRoleCreateNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "RTBFabricRoleCreateTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/RTBFabricManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RTBFabricRoleCreateNetworkInterfacePermissionActions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterfacePermission",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/RTBFabricManaged" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "RTBFabricRoleModifyTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/RTBFabricManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RTBFabricRoleTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "RTBFabricRoleDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RTBFabricRolePutMetricDataActions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/RTBFabric"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

S3StorageLensServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh S3 Storage Lens

`S3StorageLensServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 18 November 2020, 18:15 UTC
- Waktu teredit: 18 November 2020, 18.15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioAdminIAMConsolePolicy

Deskripsi: Menyediakan hak administratif awal dan pengaturan individual untuk Amazon SageMaker Unified Studio melalui Konsol Manajemen AWS dan SDK. Memungkinkan peluncuran SageMaker Unified Studio Portal.

`SageMakerStudioAdminIAMConsolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioAdminIAMConsolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Agustus 2025, 22:49 UTC
- Waktu teredit: 26 Agustus 2026, 22:47 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminIAMConsolePolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
```

```
        "iam:GetRole",
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SSMParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParametersByPath",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*"
      ]
    },
    {
      "Sid" : "DescribeEc2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables",
```

```
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateTaggedEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpc"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSubnet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSubnetInTaggedVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSubnet"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedSecurityGroupInVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateVPCEndpointInTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateInternetGateway",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway"
      ],
      "Resource" : "arn:aws:ec2:*:*:internet-gateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedNatGateway",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNatGateway"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:natgateway/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNatGatewayInTaggedSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNatGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedRouteTable",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateRouteTableInTaggedSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRouteTable"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AllocateAddress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : "arn:aws:ec2:*:*:elastic-ip/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyTaggedEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcAttribute",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AttachInternetGateway",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:AttachInternetGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateRoute",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AssociateRouteTable",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "Ec2TaggingOperations",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true",
          "ec2:CreateAction" : [
            "CreateVpc",
            "CreateSubnet",
            "CreateSecurityGroup",
            "CreateInternetGateway",
            "CreateNatGateway",
            "CreateRouteTable",
            "CreateVpcEndpoint"
          ]
        }
      }
    },
    {
      "Sid" : "Ec2TagEIP",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:elastic-ip/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AllowCFNStackCreation",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:CreateStack",
        "cloudformation:GetTemplateSummary",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack"
          ]
        }
      }
    },
    {
      "Sid" : "DeleteTaggedVpcResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpc",
        "ec2:DeleteSubnet",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteInternetGateway",
        "ec2:DetachInternetGateway",
        "ec2:DeleteNatGateway",
        "ec2:DisassociateRouteTable",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteRouteTable",
        "ec2:DeleteRoute",
        "ec2:ReleaseAddress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteTagsOnTaggedResources",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteTags",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "S3ReadCFNTemplate",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "DataZoneKMSGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueCatalogPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOApplicationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DeleteApplication"
      ],
      "Resource" : [
        "arn:aws:sso::*:application/*/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SSOKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioAdminIAMDefaultExecutionPolicy

Deskripsi: Kebijakan eksekusi administratif untuk menggunakan peran IAM dengan SageMaker Unified Studio. Memungkinkan admin menyediakan, mengelola, dan mengakses sumber daya di akun Anda (tidak termasuk akses ke sumber daya data) untuk IAM-based penggunaan SageMaker Unified Studio.

`SageMakerStudioAdminIAMDefaultExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioAdminIAMDefaultExecutionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Agustus 2025, 17:19 UTC
- Waktu teredit: 14 Juli 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminIAMDefaultExecutionPolicy`

Versi kebijakan

Versi kebijakan: v24 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataZone",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SageMakerUnifiedStudioMcp",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker-unified-studio-mcp:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:GetUser",
        "iam:ListUsers",
        "sts:AssumeRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless",
        "arn:aws:iam::*:role/aws-service-role/ops.athena.amazonaws.com/
AWSServiceRoleForAmazonAthena"
      ]
    },
    {
```

```
      "Sid" : "TagRoleAndSession",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "sts:TagSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "SageMakerSpacesDomainId"
          ]
        }
      }
    },
    {
      "Sid" : "CreateRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ]
    },
    {
      "Sid" : "AttachPolicy",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMDefaultExecutionPolicy",
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMPermissiveExecutionPolicy",
            "arn:aws:iam::aws:policy/service-role/
AmazonS3TablesLakeFormationServiceRole"
          ]
        }
      }
    },
    {
      "Sid" : "SourceIdentity",
```

```
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "PassRoleForProvisioning",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "lakeformation.amazonaws.com",
            "athena.amazonaws.com",
            "glue.amazonaws.com",
            "datazone.amazonaws.com",
            "airflow-serverless.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
        "arn:aws:iam::*:role/${aws:PrincipalTag/AmazonDataZonePassedRolePath}"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "datazone.amazonaws.com",
            "bedrock.amazonaws.com",
            "scheduler.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "elasticmapreduce.amazonaws.com",
```

```
            "redshift.amazonaws.com",
            "airflow-serverless.amazonaws.com",
            "events.amazonaws.com",
            "pods.eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "Q",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "q:Get*",
        "q:List*",
        "q:PassRequest",
        "q:SendMessage",
        "q:StartConversation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter",
        "ssm:GetParameter*",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
    },
    {
      "Sid" : "ManageSageMakerSpace",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*"
```

```
      ]
    },
    {
      "Sid" : "ResourceGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:Batch*",
        "sagemaker:DeleteTags",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sagemaker:Search",
        "sagemaker:*Endpoint*",
        "sagemaker:*Model*",
        "sagemaker:*Context*",
        "sagemaker:*Artifact*",
        "sagemaker:*Action*",
        "sagemaker:*Association*",
        "sagemaker:QueryLineage",
        "sagemaker:*InferenceComponent*",
        "sagemaker:*Job*",
        "sagemaker:*MlflowApp*",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker-mlflow:*",
        "sagemaker:*Feature*",
        "sagemaker:*Record"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateBucket",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:CreateBucket",
        "s3:DeleteBucketPolicy",
        "s3:Get*",
        "s3:Put*",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "S3List",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CrossAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:List*",
        "s3:PutObject*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*",
        "arn:aws:cloudformation:*:*:transform/*"
```

```
      ]
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "LogsAndMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "cloudwatch:GetMetricData",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:Describe*",
        "logs:Get*",
        "logs:PutLogEvents",
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LFManage",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DeregisterResource",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:ListLakeFormationOptIns",
        "lakeformation:CreateLakeFormationOptIn",
```

```
        "lakeformation:DeleteLakeFormationOptIn",
        "lakeformation:*DataCellsFilter"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:connection/*"
      ]
    },
    {
      "Sid" : "GlueLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "Glue",
      "Effect" : "Allow",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:Describe*",
        "glue:Get*",
        "glue:List*",
        "glue:NotifyEvent",
        "glue:RunStatement",
```

```
        "glue:StartCompletion",
        "glue:StopSession",
        "glue:*Resource",
        "glue:UseGlueStudio",
        "glue:*Job*",
        "glue:TestConnection",
        "glue:*DataQuality*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyForeignSessionAccess",
      "Effect" : "Deny",
      "Action" : [
        "athena:GetResourceDashboard",
        "athena:GetSession",
        "athena:GetSessionEndpoint",
        "athena:GetSessionStatus",
        "athena:StartSession",
        "athena:TerminateSession",
        "emr-serverless:*Session*",
        "emr-serverless:*Dashboard*",
        "emr-containers:*ManagedEndpoint*",
        "elasticmapreduce:*Session*",
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:GetDashboardUrl",
        "glue:GetSession",
        "glue:GetSessionEndpoint",
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
```

```
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource",
        "emr-serverless:*Resource",
        "emr-containers:*Resource",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:RemoveTags",
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "SQLWorkBench",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftData",
      "Effect" : "Allow",
      "Action" : "redshift-data:*",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RedShiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:Describe*",
        "redshift-data:ExecuteStatement",
        "redshift-data:List*",
        "redshift-serverless:GetManagedWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
        "redshift:Describe*",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Bedrock",
      "Effect" : "Allow",
      "Action" : "bedrock:*",
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Athena",
```

```
      "Effect" : "Allow",
      "Action" : [
        "athena:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowServerless",
      "Effect" : "Allow",
      "Action" : [
        "airflow-serverless:List*",
        "airflow-serverless:Get*",
        "airflow-serverless:CreateWorkflow",
        "airflow-serverless:UpdateWorkflow",
        "airflow-serverless:DeleteWorkflow",
        "airflow-serverless:StartWorkflowRun",
        "airflow-serverless:StopWorkflowRun",
        "airflow-serverless:TagResource",
        "airflow-serverless:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowMWAA",
      "Effect" : "Allow",
      "Action" : [
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:CreateWebLoginToken",
        "airflow:InvokeRestApi"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManagePrivateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy",
```

```
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageSharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        },
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*"
    },
```

```
    {
      "Sid" : "GenerateRecommendations",
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageScheduler",
      "Effect" : "Allow",
      "Action" : "scheduler:*",
      "Resource" : "*"
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnectionsAdmin",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:*",
        "codestar-connections:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3Kms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
```

```
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
```

```
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
```

```
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "CreateSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
```

```
    {
      "Sid" : "SGManage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "SGAuth",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Sid" : "SGCreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
```

```
            "AmazonDataZone*",
            "for-use-with-amazon-emr-managed-policies",
            "aws:cloudformation:*"
          ]
        }
      }
    },
    {
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "EMR",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:Get*",
        "emr-serverless:List*",
        "emr-serverless:Start*",
        "emr-serverless:Access*",
        "emr-serverless:Terminate*",
        "emr-serverless:*Resource",
        "emr-containers:*ManagedEndpoint*",
        "emr-containers:*SecurityConfiguration*",
        "emr-containers:*VirtualCluster*",
        "emr-containers:*Resource",
```

```
        "elasticmapreduce:*PersistentAppUI*",
        "elasticmapreduce:Start*",
        "elasticmapreduce:Get*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elasticmapreduce:Terminate*",
        "elasticmapreduce:*Tag*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOApplicationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication",
        "sso:PutApplicationGrant",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationAccessScope",
        "sso:UpdateApplication",
        "sso:CreateApplicationAssignment",
        "sso:DeleteApplicationAssignment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "SSOReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IdentityStoreKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "RAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:Get*",
        "ram:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMCreateResourcePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ram:RequestedResourceType" : "datazone:Domain"
        }
      }
    },
    {
      "Sid" : "RAMResourceSharePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "RAMAssociateResourceSharePermission",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionAmazonDataZoneDomain",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionAmazonDataZoneDomainFullAccessWithPortalAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceWithPortalAccess"
          ]
        }
      }
    },
    {
      "Sid" : "CanvasGeneralPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "comprehend:*",
        "textract:*",
        "rekognition:*",
        "sagemaker-data-science-assistant:*",
        "rds:DescribeDBInstances",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScalingActivities",
        "quicksight:ListNamespaces",
        "events:PutRule",
        "events:DescribeRule",
        "events:PutTargets",
        "events:TagResource",
        "events:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CanvasRedshiftAccess",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioAdminIAMPermissiveExecutionPolicy

Deskripsi: Kebijakan eksekusi administratif untuk menggunakan peran IAM dengan SageMaker Unified Studio. Memungkinkan admin untuk menyediakan, mengelola, dan mengakses sumber daya di akun lokal (termasuk akses luas ke semua API di layanan data seperti S3, Glue, CloudWatch Log, dan lainnya) untuk IAM-based penggunaan SageMaker Unified Studio.

`SageMakerStudioAdminIAMPermissiveExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioAdminIAMPermissiveExecutionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Agustus 2025, 17:19 UTC
- Waktu teredit: 14 Juli 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminIAMPermissiveExecutionPolicy`

Versi kebijakan

Versi kebijakan: v21 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:*",
        "glue:*",
        "logs:*",
        "redshift-data:*",
        "redshift-serverless:*",
        "redshift:*",
        "s3:*",
        "s3tables:*",
        "comprehend:*",
        "textract:*",
        "rekognition:*",
        "sagemaker-data-science-assistant:*",
        "rds:*",
        "quicksight:*",
        "events:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ComputeAccess",
      "Effect" : "Allow",
      "Action" : [
        "athena:*",
        "bedrock:*",
        "codewhisperer:*",
        "sagemaker-unified-studio-mcp:*",
        "datazone:*",
        "elasticmapreduce:*",
        "emr-containers:*",
        "q:*",
        "sagemaker:*",
        "sagemaker-mlflow:*",
        "scheduler:*",
        "sqlworkbench:*",
        "emr-serverless:*",
        "airflow-serverless:*",
        "airflow:*",
        "application-autoscaling:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CfnManage",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*",
        "arn:aws:cloudformation:*:*:transform/*"
      ]
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "DenyForeignSessionAccess",
      "Effect" : "Deny",
      "Action" : [
        "athena:GetResourceDashboard",
        "athena:GetSession",
        "athena:GetSessionEndpoint",
        "athena:GetSessionStatus",
        "athena:StartSession",
        "athena:TerminateSession",
        "emr-serverless:*Session*",
        "emr-serverless:*Dashboard*",
        "emr-containers:*ManagedEndpoint*",
        "elasticmapreduce:*Session*",
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:GetDashboardUrl",
        "glue:GetSession",
        "glue:GetSessionEndpoint",
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
```

```
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource",
        "emr-serverless:*Resource",
        "emr-containers:*Resource",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:RemoveTags",
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:GetUser",
        "iam:ListUsers",
        "sts:AssumeRole"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless",
        "arn:aws:iam::*:role/aws-service-role/ops.athena.amazonaws.com/
AWSServiceRoleForAmazonAthena"
      ]
    },
    {
      "Sid" : "TagRoleAndSession",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "sts:TagSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "SageMakerSpacesDomainId"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "PassRoleForProvisioning",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "lakeformation.amazonaws.com",
            "athena.amazonaws.com",
            "glue.amazonaws.com",
            "datazone.amazonaws.com",
            "airflow-serverless.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
        "arn:aws:iam::*:role/${aws:PrincipalTag/AmazonDataZonePassedRolePath}"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com",
            "datazone.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "scheduler.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "elasticmapreduce.amazonaws.com",
            "airflow-serverless.amazonaws.com",
            "pods.eks.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "CreateRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ]
    },
    {
      "Sid" : "AttachPolicy",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMDefaultExecutionPolicy",
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMPermissiveExecutionPolicy",
            "arn:aws:iam::aws:policy/service-role/
AmazonS3TablesLakeFormationServiceRole"
          ]
        }
      }
    },
    {
      "Sid" : "SourceIdentity",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter",
```

```
        "ssm:GetParameter*",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DeregisterResource",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:ListLakeFormationOptIns",
        "lakeformation:CreateLakeFormationOptIn",
        "lakeformation:DeleteLakeFormationOptIn",
        "lakeformation:*DataCellsFilter"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets",
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManagePrivateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageSharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        },
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "RedshiftSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*"
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnections",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:*",
        "codestar-connections:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3Kms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
```

```
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
```

```
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
```

```
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "CreateSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
```

```
    {
      "Sid" : "SGManage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "SGAuth",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Sid" : "SGCreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
```

```
            "AmazonDataZone*",
            "for-use-with-amazon-emr-managed-policies",
            "aws:cloudformation:*"
          ]
        }
      }
    },
    {
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "SSOApplicationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication",
        "sso:PutApplicationGrant",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationAccessScope",
        "sso:UpdateApplication",
        "sso:CreateApplicationAssignment",
        "sso:DeleteApplicationAssignment"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "SSOReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IdentityStoreKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "RAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:Get*",
        "ram:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMCreateResourcePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:RequestedResourceType" : "datazone:Domain"
        }
      }
    },
    {
      "Sid" : "RAMResourceSharePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "RAMAssociateResourceSharePermission",
```

```
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionAmazonDataZoneDomain",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionAmazonDataZoneDomainFullAccessWithPortalAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceWithPortalAccess"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioAdminProjectUserRolePolicy

Deskripsi: Kebijakan IAM ini memberikan peran IAM akses penuh ke Katalog Data AWS Glue (metadata) dan Amazon S3 (data aktual) untuk operasi data lake, dengan akses yang dicakup oleh akun, dan tag peran.

`SageMakerStudioAdminProjectUserRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioAdminProjectUserRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Juli 2025, 20:52 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminProjectUserRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueDatalakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:GetCatalogImportStatus",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
```

```
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:ListTableOptimizerRuns",
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:GetCatalogs",
        "glue:GetCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aws:PrincipalTag/BootstrappedServices" : "*glue*"
        }
      }
    },
    {
      "Sid" : "GlueCatalogDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase"
```

```
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aws:PrincipalTag/BootstrappedServices" : "*glue*"
        }
      }
    },
    {
      "Sid" : "DataAccessPermissionsForS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aws:PrincipalTag/BootstrappedServices" : "*glue*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioBedrockAgentServiceRolePolicy

Deskripsi: Mengizinkan Amazon Bedrock Agents mengakses model Amazon Bedrock dan sumber daya lain yang melekat pada agen di SageMaker Studio.

`SageMakerStudioBedrockAgentServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioBedrockAgentServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 13 Februari 2025, 23:37 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockAgentServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAppInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
```

```
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockModelInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockApplyGuardrailPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ApplyGuardrail",
      "Resource" : "arn:aws:bedrock:*:*:guardrail/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockRetrieveAndGeneratePermissions",
      "Effect" : "Allow",
```

```
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaInvokeFunctionInProjectPermissions",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockRetrievePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:Retrieve",
      "Resource" : "arn:aws:bedrock:*:*:knowledge-base/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "S3GetObjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAttributes",
        "s3:GetObjectAttributes"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
```

```
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "BedrockGuardrailKmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:guardrail-id" : "false"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioBedrockChatAgentUserRolePolicy

Deskripsi: Menyediakan akses ke konfigurasi aplikasi agen obrolan Amazon Bedrock dan agen Amazon Bedrock di SageMaker Studio.

`SageMakerStudioBedrockChatAgentUserRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioBedrockChatAgentUserRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 13 Februari 2025, 23:52 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockChatAgentUserRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockGetAgentAliasPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:GetAgentAlias",
      "Resource" : "arn:aws:bedrock:*:*:agent-alias/${aws:PrincipalTag/AgentId}/
${aws:PrincipalTag/AgentAliasId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeAgent",
      "Resource" : "arn:aws:bedrock:*:*:agent-alias/${aws:PrincipalTag/AgentId}/
${aws:PrincipalTag/AgentAliasId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockGetAndListAgentMetadataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
```

```
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgentVersions"
      ],
      "Resource" : "arn:aws:bedrock:*:*:agent/${aws:PrincipalTag/AgentId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "S3ListAppDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/${aws:PrincipalTag/AppDefinitionPath}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AppDefinitionPath" : ""
        }
      }
    },
    {
      "Sid" : "S3GetAppDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/AppDefinitionPath}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AppDefinitionPath" : ""
        }
      }
    },
    {
      "Sid" : "S3ListDataSourcePermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/${aws:PrincipalTag/DataSourcePath}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/DataSourcePath" : ""
        }
      }
    },
    {
      "Sid" : "S3GetDataSourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/DataSourcePath}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
```

```
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/DataSourcePath" : ""
        }
      }
    },
    {
      "Sid" : "BedrockAgentKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:agent/${aws:PrincipalTag/AgentId}"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioBedrockEvaluationJobServiceRolePolicy

Deskripsi: Mengizinkan Amazon Bedrock mengakses model dan kumpulan data Amazon Bedrock untuk pekerjaan evaluasi di Studio. SageMaker

`SageMakerStudioBedrockEvaluationJobServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioBedrockEvaluationJobServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: Februari 14, 2025, 00:37 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockEvaluationJobServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockEvaluationInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:GetInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeModelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "BedrockModelInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateModelInvocationJob",
        "bedrock:StopModelInvocationJob",
        "bedrock:GetProvisionedModelThroughput"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3GetBucketLocationPermissions",
      "Effect" : "Allow",
      "Action" : "s3:GetBucketLocation",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : ""
        }
      }
    },
    {
      "Sid" : "S3ListBucketPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
        },
```

```
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "S3EvaluationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/${aws:PrincipalTag/
AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "KmsDescribeKeyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioBedrockFlowServiceRolePolicy

Deskripsi: Mengizinkan Amazon Bedrock Flows mengakses model Amazon Bedrock dan sumber daya lain yang terpasang pada aliran di SageMaker Studio.

`SageMakerStudioBedrockFlowServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioBedrockFlowServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Februari 2025, 00:07 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockFlowServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockPromptPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:GetPrompt",
      "Resource" : "arn:aws:bedrock:*:*:prompt/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
```

```
      "Sid" : "BedrockKnowledgeBasePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:Retrieve",
      "Resource" : "arn:aws:bedrock:*:*:knowledge-base/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockGuardrailPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ApplyGuardrail",
      "Resource" : "arn:aws:bedrock:*:*:guardrail/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AllowBedrockRetrieveAndGeneratePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLambdaInvokeFunctionInProjectPermissions",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
```

```
    {
      "Sid" : "AllowBedrockApplicationInferenceProfileAccessInProjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AllowBedrockInvokeModelAccessWithInferenceProfilePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeAgent",
      "Resource" : "arn:aws:bedrock:*:*:agent-alias/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
```

```
      "Sid" : "BedrockPromptKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock-prompts:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:prompt/*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockGuardrailKmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:guardrail-id" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockAgentKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
```

```
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:agent/*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioBedrockFunctionExecutionRolePolicy

Deskripsi: Men AWS gizinkan Lambda mengakses konfigurasi komponen fungsi Amazon Bedrock di SageMaker Studio.

`SageMakerStudioBedrockFunctionExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioBedrockFunctionExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 25 Februari 2025, 03:52 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockFunctionExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecretsManagerReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "KMSSameAccountBedrockViaSecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:*:
${aws:PrincipalAccount}:secret:amazon-bedrock*"
```

```
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy

Deskripsi: Menyediakan akses untuk mengonfigurasi penyimpanan vektor dan basis pengetahuan Amazon Bedrock di SageMaker Studio.

`SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 25 Februari 2025, 03:37 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OpenSearchServerlessPermissions",
      "Effect" : "Allow",
      "Action" : "aoss:APIAccessAll",
      "Resource" : "arn:aws:aoss:*:*:collection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aoss:collection" : "bedrock*"
        }
      }
    },
    {
      "Sid" : "BedrockKnowledgeBasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetIngestionJob",
        "bedrock:ListIngestionJobs",
        "bedrock:StartIngestionJob"
      ],
      "Resource" : "arn:aws:bedrock:*:*:knowledge-base/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy

Deskripsi: Mengizinkan Basis Pengetahuan Amazon Bedrock mengakses model Amazon Bedrock dan sumber data di SageMaker Studio.

`SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 25 Februari 2025, 02:52 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAppInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockModelInvocationPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "OpenSearchServerlessPermissions",
      "Effect" : "Allow",
      "Action" : "aoss:APIAccessAll",
      "Resource" : "arn:aws:aoss:*:*:collection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aoss:collection" : "bedrock*"
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "s3:prefix" : [
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}",
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
          ]
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "AccessDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
```

```
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "VectorStoresKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "neptune-graph.*.amazonaws.com",
            "s3vectors.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "VectorStoresKmsDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
```

```
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "neptune-graph.*.amazonaws.com",
            "s3vectors.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "NeptuneGraphDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:GetGraph",
        "neptune-graph:DeleteDataViaQuery",
        "neptune-graph:WriteDataViaQuery",
        "neptune-graph:ReadDataViaQuery"
      ],
      "Resource" : "arn:aws:neptune-graph:*:*:graph/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "S3VectorsDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3vectors:GetVectorBucket",
        "s3vectors:GetIndex",
        "s3vectors:PutVectors",
        "s3vectors:GetVectors",
        "s3vectors:ListVectors",
        "s3vectors:QueryVectors",
        "s3vectors:DeleteVectors"
      ],
      "Resource" : "arn:aws:s3vectors:*:*:bucket/amazon-bedrock-ide-${aws:PrincipalTag/
AmazonDataZoneProject}*",
```

```
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockKnowledgeBaseKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:bedrock:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:knowledge-base/*"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "SqlWorkbenchAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:GetSqlRecommendations",
        "sqlworkbench:PutSqlGenerationContext",
        "sqlworkbench:GetSqlGenerationContext",
        "sqlworkbench:DeleteSqlGenerationContext"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockGenerateQueryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioBedrockPromptUserRolePolicy

Deskripsi: Menyediakan akses ke prompt Amazon Bedrock dan konfigurasinya di SageMaker Studio.

`SageMakerStudioBedrockPromptUserRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioBedrockPromptUserRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: Februari 14, 2025, 00:22 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockPromptUserRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockPromptReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:GetPrompt",
      "Resource" : "arn:aws:bedrock:*:*:prompt/${aws:PrincipalTag/PromptId}:
${aws:PrincipalTag/PromptVersion}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
```

```
    {
      "Sid" : "S3ListPromptDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/${aws:PrincipalTag/PromptDefinitionPath}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/PromptDefinitionPath" : ""
        }
      }
    },
    {
      "Sid" : "S3GetPromptDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/PromptDefinitionPath}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/PromptDefinitionPath" : ""
        }
      }
    },
    {
      "Sid" : "BedrockPromptKmsPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock-prompts:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:prompt/${aws:PrincipalTag/PromptId}"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioDomainExecutionRolePolicy

Deskripsi: Kebijakan ini digunakan oleh Amazon SageMaker Studio untuk membuat katalog, menemukan, mengatur, berbagi, dan menganalisis data di domain Amazon SageMaker Studio.

`SageMakerStudioDomainExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioDomainExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 November 2024, 21:56 UTC
- Waktu teredit: 12 Agustus 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioDomainExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v23 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataZonePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:AddEntityOwner",
        "datazone:AddPolicyGrant",
        "datazone:AssociateGovernedTerms",
        "datazone:BatchGetAttributesMetadata",
        "datazone:BatchPutAttributesMetadata",
        "datazone:BatchUpdateNotifications",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetFilter",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateConnection",
        "datazone:CreateDataProduct",
        "datazone:CreateDataProductRevision",
        "datazone:CreateDataSource",
        "datazone:CreateDomainUnit",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateRule",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetFilter",
        "datazone:DeleteAssetType",
        "datazone:DeleteConnection",
        "datazone:DeleteDataProduct",
        "datazone:DeleteDataSource",
        "datazone:DeleteDomainUnit",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
```

```
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteRule",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
        "datazone:DeleteTimeSeriesDataPoints",
        "datazone:DisassociateGovernedTerms",
        "datazone:GetAsset",
        "datazone:GetAssetFilter",
        "datazone:GetAssetType",
        "datazone:GetConnection",
        "datazone:GetCurrentEffectivePolicy",
        "datazone:GetDataProduct",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDesignation",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetLineageNode",
        "datazone:GetListing",
        "datazone:GetMetadataGenerationRun",
        "datazone:GetProject",
        "datazone:GetRule",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetTimeSeriesDataPoint",
        "datazone:GetUpdateEligibility",
        "datazone:GetUserProfile",
```

```
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetFilters",
        "datazone:ListAssetRevisions",
        "datazone:ListConnections",
        "datazone:ListDataProductRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListDesignations",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListLineageNodeHistory",
        "datazone:ListMetadataGenerationRuns",
        "datazone:ListNotifications",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListRules",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:ListWarehouseMetadata",
        "datazone:QueryGraph",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RemoveEntityOwner",
        "datazone:RemovePolicyGrant",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
```

```
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateConnection",
        "datazone:UpdateDataSource",
        "datazone:UpdateDomainUnit",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
        "datazone:UpdateRule",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMResourceShareStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonQPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:PassRequest",
        "q:GetIdentityMetadata",
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "SSMGetParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q/${aws:PrincipalTag/datazone-
domainId}*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/${aws:PrincipalTag/datazone-
domainId}/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetCodeConnectionsPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection",
        "codeconnections:GetHost",
        "codestar-connections:GetConnection",
        "codestar-connections:GetHost"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "false"
        },
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "ListCodeConnectionsPermissionsStatement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codestar-connections:ListConnections",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "UseCodeConnectionsPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection",
        "codestar-connections:UseConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "false"
        },
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "ProjectProfilePermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:GetProjectProfile",
        "datazone:ListProjectProfiles"
      ],
      "Resource" : "arn:aws:datazone:*:*:domain/*"
    },
    {
      "Sid" : "AccountPoolPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:GetAccountPool",
        "datazone:ListAccountPools",
        "datazone:ListAccountsInAccountPool"
      ],
      "Resource" : "arn:aws:datazone:*:*:domain/*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioDomainServiceRolePolicy

Deskripsi: Peran layanan untuk tindakan tingkat domain di portal yang dilakukan oleh Amazon SageMaker Studio.

`SageMakerStudioDomainServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioDomainServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 November 2024, 21:56 UTC
- Waktu teredit: 20 November 2024, 21:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioDomainServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SSMGetParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/profiles/*"
      ]
    },
    {
      "Sid" : "UseKMSKeyPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "true"
        },
        "Null" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm.*.amazonaws.com",
          "kms:EncryptionContext:PARAMETER_ARN" : "arn:aws:ssm:*:*:parameter/amazon/
datazone/profiles*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioEMRContainersSystemNamespaceRolePolicy

Deskripsi: Amazon SageMaker Studio membuat peran IAM bagi pengguna proyek untuk melakukan analitik data, kecerdasan buatan, dan tindakan pembelajaran mesin, dan menggunakan kebijakan ini saat membuat peran ini untuk menentukan izin yang terkait dengan EMR.

`SageMakerStudioEMRContainersSystemNamespaceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioEMRContainersSystemNamespaceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 23 Oktober 2025, 18:34 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRContainersSystemNamespaceRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AssumeProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "TagSessionProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "sts:TagSession"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "LakeFormationAuthorizedCaller"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/LakeFormationAuthorizedCaller" : "EMR on EKS Engine",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
```

```
    {
      "Sid" : "SetContextProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "ForAllValues:ArnEquals" : {
          "sts:RequestContextProviders" : [
            "arn:aws:iam::aws:contextProvider/IdentityCenter"
          ]
        },
        "Null" : {
          "sts:RequestContextProviders" : "false"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioEMRInstanceRolePolicy

Deskripsi: Amazon SageMaker Studio membuat peran IAM bagi pengguna proyek untuk melakukan analitik data, kecerdasan buatan, dan tindakan pembelajaran mesin, dan menggunakan kebijakan ini saat membuat peran ini untuk menentukan izin yang terkait dengan EMR.

`SageMakerStudioEMRInstanceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioEMRInstanceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 27 Februari 2025, 00:22 UTC
- Waktu teredit: 01 Juni 2026, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRInstanceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessCertificateLocationS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/certificate_location/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : ""
        },
        "Null" : {
```

```
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessPatchingRPMsS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::default-env-blueprint-*/*",
        "arn:aws:s3:::awssmuscompute-blueprint-bucket-*/*",
        "arn:aws:s3:*:*:accesspoint/env-blueprint-accesspoint*",
        "arn:aws:s3:*:*:accesspoint/env-partner-blueprint-accesspoint*"
      ],
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : [
            "arn:aws:s3:*:*:accesspoint/env-blueprint-accesspoint",
            "arn:aws:s3:*:*:accesspoint/env-partner-blueprint-accesspoint"
          ]
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessBootstrapActionScriptS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/AmazonDataZoneScopeName}/sys/emr/bootstrap-script/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AmazonDataZoneScopeName" : ""
        },
        "Null" : {
```

```
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRClusterLogUploadS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:PutObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/AmazonDataZoneScopeName}/sys/emr/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AmazonDataZoneScopeName" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRRuntimeRoleAssumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "LakeFormationAuthorizedCaller"
          ]
        },
        "StringEquals" : {
```

```
          "iam:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EMRKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGenerateDataKeyForEbsEncryption",
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioEMRServiceRolePolicy

Deskripsi: Amazon SageMaker Studio membuat peran IAM bagi pengguna proyek untuk melakukan analitik data, kecerdasan buatan, dan tindakan pembelajaran mesin, dan menggunakan kebijakan ini saat membuat peran ini untuk menentukan izin yang terkait dengan EMR.

`SageMakerStudioEMRServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioEMRServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 31 Januari 2025, 19:52 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PassRoleToEMREC2InstanceRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/datazone_emr_ec2_instance_role_
${aws:PrincipalTag/AmazonDataZoneProject}_${aws:PrincipalTag/
AmazonDataZoneEnvironment}",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AmazonDataZoneEnvironment" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CreateInNetworkForSharedSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:Vpc" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}"
        }
```

```
      }
    },
    {
      "Sid" : "EMRKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGenerateDataKeyForEbsEncryption",
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDescribeKeyForLogPusherCMK",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioFullAccess

Deskripsi: Kebijakan ini menyediakan akses penuh ke Amazon SageMaker Unified Studio melalui konsol SageMaker manajemen Amazon.

`SageMakerStudioFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2024, 00:06 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioFullAccess`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "iam:ListPolicies",
        "sso:DescribeRegisteredRegions",
        "s3:ListAllMyBuckets",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "secretsmanager:ListSecrets",
        "iam:ListUsers",
        "glue:GetDatabases",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codewhisperer:ListProfiles",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListFoundationModels",
        "bedrock:ListTagsForResource",
```

```
        "aoss:ListSecurityPolicies",
        "quicksight:DescribeAccountSubscription",
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BucketReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "ReadManagedBlueprintTemplatesStatement",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::default-env-blueprint-*/*",
        "arn:aws:s3:*:*:accesspoint/env-blueprint-accesspoint*"
      ],
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/env-blueprint-
accesspoint"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CreateBucketStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-datazone*",
```

```
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "ConfigureBucketStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketCORS",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PutObjectStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RamCreateResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "datazone:Domain"
        }
      }
    },
    {
      "Sid" : "RamResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:RejectResourceShareInvitation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "RamResourceReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations",
        "ram:ListResourceSharePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RamAssociateResourceSharePermissionStatement",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionAmazonDataZoneDomain",
```

```
            "arn:aws:ram::aws:permission/
AWSRAMPermissionAmazonDataZoneDomainFullAccessWithPortalAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceWithPortalAccess"
          ]
        }
      }
    },
    {
      "Sid" : "IAMPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMGetPolicyStatement",
      "Effect" : "Allow",
      "Action" : "iam:GetPolicy",
      "Resource" : [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneRedshiftAccessPolicy*"
      ]
    },
    {
      "Sid" : "DataZoneTagOnCreateDomainProjectTags",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
```

```
            "AmazonDataZoneProject"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "DataZoneTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "CreateSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "ConnectionStatement",
      "Effect" : "Allow",
```

```
      "Action" : [
        "codeconnections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "TagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:TagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:host/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "for-use-with-all-datazone-projects"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "UntagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UntagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:host/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "for-use-with-all-datazone-projects"
        }
      }
    },
```

```
    {
      "Sid" : "SSMParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParametersByPath",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/profiles*"
      ]
    },
    {
      "Sid" : "UseKMSKeyPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "true"
        },
        "Null" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetSecurityPolicy",
        "aoss:CreateSecurityPolicy"
      ],
      "Resource" : [
```

```
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "bedrock-ide-*"
        }
      }
    },
    {
      "Sid" : "GetFoundationModelStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
      ]
    },
    {
      "Sid" : "GetInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*",
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ]
    },
    {
      "Sid" : "ApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "TagApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:DeleteInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
    {
      "Sid" : "ModelAccessUseCaseStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetUseCaseForModelAccess",
        "bedrock:PutUseCaseForModelAccess"
      ],
      "Resource" : [
```

```
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioProjectProvisioningRolePolicy

Deskripsi: Amazon SageMaker Studio menggunakan kebijakan ini untuk menyediakan dan mengelola sumber daya di akun Anda.

`SageMakerStudioProjectProvisioningRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioProjectProvisioningRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 November 2024, 21:58 UTC
- Waktu teredit: 22 September 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioProjectProvisioningRolePolicy`

Versi kebijakan

Versi kebijakan: v83 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CfnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnMng",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:UpdateStack"
      ],
```

```
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnDelete",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Discovery",
      "Effect" : "Allow",
      "Action" : [
        "airflow:GetEnvironment",
        "bedrock:ListEvaluationJobs",
        "cloudformation:ValidateTemplate",
        "codecommit:ListRepositories",
        "eks:DescribeCluster",
        "elasticmapreduce:CreateSecurityConfiguration",
        "elasticmapreduce:DeleteSecurityConfiguration",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "glue:DescribeConnectionType",
        "glue:ListConnectionTypes",
        "glue:*GlueIdentityCenterConfiguration",
        "iam:ListPolicies",
```

```
        "logs:DescribeLogGroups",
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeDataShares",
        "redshift:DescribeDataSharesForConsumer",
        "redshift:GetResourcePolicy",
        "sagemaker:DescribeDomain",
        "sagemaker:ListDomains",
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LFMng",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:ListPermissions",
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:BatchGrantPermissions",
        "lakeformation:ListResources",
        "lakeformation:DescribeResource",
        "lakeformation:*LakeFormationIdentityCenterConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DzTemplate",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "DzCfTemplate",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::amazon-sagemaker-cf-templates*/*"
    },
    {
      "Sid" : "DataZoneEnvironmentResources",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*Connection",
        "datazone:*DataSource",
        "datazone:*SubscriptionTarget"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CcCreate",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CreateRepository",
        "codecommit:TagResource"
      ],
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CcDelete",
```

```
      "Effect" : "Allow",
      "Action" : [
        "codecommit:DeleteRepository",
        "codecommit:UntagResource",
        "codecommit:UpdateRepositoryEncryptionKey",
        "codecommit:PutRepositoryTriggers"
      ],
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CcAccess",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GetBranch",
        "codecommit:CreateCommit",
        "codecommit:GetRepository",
        "codecommit:GetFile"
      ],
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CcKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "Null" : {
          "kms:EncryptionContext:aws:codecommit:id" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "codecommit.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetIamRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ]
    },
    {
      "Sid" : "IAMMng",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrockExecution*",
        "arn:aws:iam::*:role/BedrockStudio*",
        "arn:aws:iam::*:role/AmazonBedrockConsumptionRole*",
        "arn:aws:iam::*:role/AmazonBedrockEvaluation*"
      ],
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        }
      }
    },
    {
      "Sid" : "IamDzMng",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        }
      }
    },
    {
      "Sid" : "RoleCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "IamMng",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePolicy",
            "arn:aws:iam::aws:policy/SageMakerStudioProjectRoleMachineLearningPolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioEMRContainersSystemNamespaceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRServiceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioEMRInstanceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2",
            "arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicyForSessions",
            "arn:aws:iam::aws:policy/service-role/
AmazonS3TablesLakeFormationServiceRole",
            "arn:aws:iam::aws:policy/AmazonSageMakerPartnerAppsFullAccess",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamMngAdmin",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
```

```
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioAdminProjectUserRolePolicy",
            "arn:aws:iam::aws:policy/SageMakerStudioAdminIAMDefaultExecutionPolicy"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneAdminProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamMngBR",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonBedrock*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockAgentServiceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockChatAgentUserRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockFlowServiceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockFunctionExecutionRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockPromptUserRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockEvaluationJobServiceRolePolicy"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "IamTag",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/datazone_s3tables_*",
        "arn:aws:iam::*:role/datazone-partner-apps-*",
        "arn:aws:iam::*:role/datazone_redshift_serverless_admin_role_*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*",
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "BootstrappedServices",
            "AmazonBedrockManaged",
            "RedshiftDb*",
            "EnableAmazonBedrockPermissions",
            "EnableAmazonBedrockIDEPermissions",
            "EnableGlueWorkloadsPermissions",
            "EnableSageMakerMLWorkloadsPermissions",
            "DomainBucketName",
            "KmsKeyId",
            "DomainKmsKeyId",
            "DefaultGlueCatalogKmsKeyId",
            "LogGroupName",
            "RoleName",
            "vpcArn",
            "VpcId",
            "CreatedForUseWithSageMakerStudio",
            "SageMakerStudioQueryExecutionRole",
            "SageMakerSpacesDomainId"
          ]
        },
        "Null" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AdminProjectTagRoleMng",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZoneScopeName",
            "BootstrappedServices",
            "AmazonDataZoneAdminProject"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamTagBR",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonBedrock*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged",
            "DomainBucketName",
            "KmsKeyId",
            "AgentId",
```

```
            "AgentAliasId",
            "AppDefinitionPath",
            "DataSourcePath",
            "PromptId",
            "PromptVersion",
            "PromptDefinitionPath",
            "OpenSearchServerlessCollectionId"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamTagRS",
      "Effect" : "Allow",
      "Action" : "iam:TagRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "RedshiftDb*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        }
      }
    },
    {
      "Sid" : "IamTagEMR",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_emr_service_role_*",
        "arn:aws:iam::*:role/datazone_emr_ec2_instance_role_*",
        "arn:aws:iam::*:role/datazone_emr_containers_system_namespace_role_*"
```

```
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "DataZone*",
            "for-use-with-amazon-emr-managed-policies",
            "DomainBucketName",
            "KmsKeyId",
            "VpcId"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        }
      }
    },
    {
      "Sid" : "IamUntag",
      "Effect" : "Allow",
      "Action" : "iam:UntagRole",
      "Resource" : "arn:aws:iam::*:role/datazone_usr_role_*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "EnableAmazonBedrockIDEPermissions"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "MngRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
```

```
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DzMngRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:UpdateAssumeRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/datazone_emr_*",
        "arn:aws:iam::*:role/datazone-partner-apps-*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/datazone_s3tables_*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamAttach",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        }
      }
```

```
    },
    {
      "Sid" : "IamDetach",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*"
      ]
    },
    {
      "Sid" : "DzMngPolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeletePolicy",
        "iam:CreatePolicy",
        "iam:ListPolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:CreatePolicyVersion",
        "iam:ListPolicyVersions",
        "iam:DeletePolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/datazone*",
        "arn:aws:iam::*:policy/connector-manage-access-policy*",
        "arn:aws:iam::*:policy/SageMakerStudioQueryExecutionRolePolicy"
      ]
    },
    {
      "Sid" : "InstanceProfile",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/
datazone_emr_ec2_instance_profile_*"
    },
```

```
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com",
            "glue.amazonaws.com"
          ],
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "airflow.amazonaws.com",
            "athena.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForDZ",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "datazone.amazonaws.com",
            "sagemaker.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "PassRoleForGlue",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/datazone_s3tables_*",
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerQueryExecution"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForEmr",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_emr_service_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticmapreduce.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForEmrIP",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_emr_ec2_instance_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
```

```
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleToBR",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassRoleToLambda",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AossSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
observability.aoss.amazonaws.com/AWSServiceRoleForAmazonOpenSearchServerless",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "observability.aoss.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "GlueDb",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/s3tablescatalog",
        "arn:aws:glue:*:*:catalog/s3tablescatalog/*",
        "arn:aws:glue:*:*:database/s3tablescatalog/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnGlueDb",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueDbTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
```

```
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueDbDelete",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteDatabase"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueConnTag",
```

```
      "Effect" : "Allow",
      "Action" : "glue:GetConnection",
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/datazone-glue-network-connection-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueConnMng",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection",
        "glue:DeleteConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/datazone-glue-network-connection-*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueConnections",
      "Effect" : "Allow",
      "Action" : [
        "glue:PassConnection",
        "glue:GetConnections",
        "glue:GetTags"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "AthenaConnection",
      "Effect" : "Allow",
      "Action" : [
        "athena:CreateDataCatalog"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "GetConnection",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "ConnectionTag",
      "Effect" : "Allow",
      "Action" : [
        "athena:TagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:datacatalog/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "federated_athena*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "CreateConn",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngConnection",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteConnection",
        "glue:UpdateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngCatalogConn",
      "Effect" : "Allow",
```

```
      "Action" : [
        "glue:DeleteConnection",
        "glue:UpdateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "kms:EncryptionContext:glue_catalog_id" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "glue.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetDataCatalogEncSett",
      "Effect" : "Allow",
      "Action" : "glue:GetDataCatalogEncryptionSettings",
      "Resource" : "arn:aws:glue:*:*:catalog",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "Repo",
      "Effect" : "Allow",
      "Action" : [
        "serverlessrepo:GetCloudFormationTemplate",
        "serverlessrepo:CreateCloudFormationTemplate"
      ],
      "Resource" : [
        "arn:aws:serverlessrepo:*:*:applications/Athena*"
      ]
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/athena-federation-repository*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CfnChangeSet",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:transform/*"
      ]
    },
    {
```

```
      "Sid" : "LambdaMng",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaGet",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : [
            "athena.amazonaws.com",
            "cloudformation.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:TagResource"
```

```
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "aws:cloudformation:*",
            "federated_athena*",
            "lambda:createdBy"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaS3Get",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::awsserverlessrepo*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:CalledViaLast" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3List",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "Null" : {
          "s3:prefix" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3Create",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketCORS",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:DeleteBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "Cfn",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/athenafederatedcatalog*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/federated_athena_datacatalog" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "AthenaDC",
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteDataCatalog",
        "athena:GetDataCatalog",
        "athena:UpdateDataCatalog"
      ],
      "Resource" : "arn:aws:athena:*:*:datacatalog/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerQueryExecution",
        "arn:aws:iam::*:role/datazone_s3tables_*"
      ]
    },
```

```
    {
      "Sid" : "S3tPassConn",
      "Effect" : "Allow",
      "Action" : [
        "glue:PassConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/aws:s3tables"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "lakeformation:EnabledOnlyForMetaDataAccess" : "true"
        }
      }
    },
    {
      "Sid" : "GlueCatalogCreate",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueCatalogMgmt",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:UpdateCatalog",
        "glue:DeleteCatalog",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RSMng",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateNamespace",
        "redshift-serverless:CreateWorkgroup",
        "redshift-serverless:DeleteNamespace",
        "redshift-serverless:DeleteWorkgroup",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshotcopyconfiguration/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftDataShare",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AssociateDataShareConsumer",
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:datashare:*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "redshift-serverless.amazonaws.com",
            "glue.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging"
      ],
      "Resource" : "arn:aws:s3:::redshift-staging-bucket-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "RedshiftTag",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:TagResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CreateSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "true"
        }
      }
    },
    {
      "Sid" : "SGAuth",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SGMng",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "SGRevoke",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "TagEc2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "for-use-with-amazon-emr-managed-policies",
            "aws:cloudformation:*"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2Mng",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateLG",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
```

```
        "arn:aws:logs:*:*:log-group:datazone-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/amazon-bedrock-ide-*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LGRetention",
      "Effect" : "Allow",
      "Action" : "logs:PutRetentionPolicy",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:datazone-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/amazon-bedrock-ide-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngLG",
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogGroup",
        "logs:UntagResource",
        "logs:DeleteRetentionPolicy",
        "logs:GetDataProtectionPolicy",
        "logs:PutDataProtectionPolicy",
        "logs:DeleteDataProtectionPolicy",
        "logs:AssociateKmsKey",
        "logs:DisassociateKmsKey",
```

```
        "logs:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:datazone-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/amazon-bedrock-ide-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AthenaMng",
      "Effect" : "Allow",
      "Action" : [
        "athena:CreateWorkGroup",
        "athena:TagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "aws:cloudformation:*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AthenaWGDelete",
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteWorkGroup",
```

```
        "athena:UpdateWorkGroup",
        "athena:UntagResource",
        "athena:GetWorkGroup"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftCreate",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateNamespace",
        "redshift-serverless:CreateWorkgroup",
        "redshift-serverless:TagResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagRSS",
      "Effect" : "Allow",
```

```
      "Action" : [
        "redshift-serverless:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:ResourceTag/CreatedBy" : "false"
        }
      }
    },
    {
      "Sid" : "SecretProject",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "SecretAll",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "TagSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "CreatedBy"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:ResourceTag/CreatedBy" : "false",
          "aws:TagKeys" : "false"
        }
      }
    },
    {
      "Sid" : "SecretKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SsoKms",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IdStoreKms",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateSLR",
```

```
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/emr-containers.amazonaws.com/
AWSServiceRoleForAmazonEMRContainers",
        "arn:aws:iam::*:role/aws-service-role/ops.athena.amazonaws.com/
AWSServiceRoleForAmazonAthena"
      ]
    },
    {
      "Sid" : "RssMng",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-serverless:GetCredentials",
        "redshift-serverless:UntagResource",
        "redshift-serverless:UpdateNamespace",
        "redshift-serverless:UpdateWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "RedshiftKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:redshift-serverless:arn" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "redshift-serverless.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "BRSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "RedshiftSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagRsSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "Redshift",
            "aws:secretsmanager:*",
            "aws:redshift-serverless:*",
            "AmazonDataZone*",
            "datazone.rs.workgroup"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "TagSMD",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
        "arn:aws:sagemaker:*:*:mlflow-app/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagSMDForUpdate",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateDomain",
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
        "arn:aws:sagemaker:*:*:mlflow-app/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngSMD",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:UpdateDomain",
        "sagemaker:DeleteDomain"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:domain/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SMApp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:AddTags",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DeleteSpace",
      "Effect" : "Allow",
      "Action" : "sagemaker:DeleteSpace",
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "DeleteUserProfile",
      "Effect" : "Allow",
      "Action" : "sagemaker:DeleteUserProfile",
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EmrSCreate",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:CreateApplication",
        "emr-serverless:TagResource"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EmrSMng",
      "Effect" : "Allow",
```

```
      "Action" : [
        "emr-serverless:DeleteApplication",
        "emr-serverless:GetApplication",
        "emr-serverless:StopApplication",
        "emr-serverless:UpdateApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EmrSEc2Eni",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "ops.emr-serverless.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EmrSEc2Subnet",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "ops.emr-serverless.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "MLFlowCreate",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateMlflowTrackingServer",
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MLFlowDescribe",
      "Effect" : "Allow",
      "Action" : "sagemaker:DescribeMlflowTrackingServer",
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*"
    },
    {
      "Sid" : "MLFlowDelete",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteMlflowTrackingServer"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MLFlowServerlessCreate",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateMlflowApp"
```

```
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-app/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "MLFlowServerlessDescribeDelete",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteMlflowApp",
        "sagemaker:DescribeMlflowApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-app/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AossMng",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetAccessPolicy",
        "aoss:CreateAccessPolicy",
        "aoss:DeleteAccessPolicy",
        "aoss:UpdateAccessPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "aoss:collection" : "bedrock-ide-*",
          "aoss:index" : "bedrock-ide-*"
        }
      }
    },
    {
      "Sid" : "MngAossPolicies",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetSecurityPolicy",
```

```
        "aoss:CreateSecurityPolicy",
        "aoss:DeleteSecurityPolicy",
        "aoss:UpdateSecurityPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "aoss:collection" : "bedrock-ide-*"
        }
      }
    },
    {
      "Sid" : "GetAoss",
      "Effect" : "Allow",
      "Action" : "aoss:BatchGetCollection",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AossCollections",
      "Effect" : "Allow",
      "Action" : [
        "aoss:CreateCollection",
        "aoss:UpdateCollection",
        "aoss:DeleteCollection",
        "aoss:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngNeptune",
      "Effect" : "Allow",
```

```
      "Action" : [
        "neptune-graph:CreateGraph",
        "neptune-graph:UpdateGraph",
        "neptune-graph:DeleteGraph",
        "neptune-graph:ListGraphs",
        "neptune-graph:GetGraph"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "S3VectorsMng",
      "Effect" : "Allow",
      "Action" : [
        "s3vectors:CreateVectorBucket",
        "s3vectors:DeleteVectorBucket",
        "s3vectors:ListVectorBuckets",
        "s3vectors:GetVectorBucket",
        "s3vectors:CreateIndex",
        "s3vectors:DeleteIndex",
        "s3vectors:ListIndexes",
        "s3vectors:GetIndex"
      ],
      "Resource" : "arn:aws:s3vectors:*:*:bucket/amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagNeptune",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:TagResource"
      ],
      "Resource" : "arn:aws:neptune-graph:*:*:graph/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
```

```
            "AmazonDataZone*",
            "AmazonBedrock*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "GetS3GenAI",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/dzd*/*/genAI/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetBR",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetAgent",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetGuardrail",
        "bedrock:GetPrompt",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BRMng",
```

```
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateAgent",
        "bedrock:UpdateAgent",
        "bedrock:PrepareAgent",
        "bedrock:DeleteAgent",
        "bedrock:ListAgentAliases",
        "bedrock:GetAgentAlias",
        "bedrock:CreateAgentAlias",
        "bedrock:UpdateAgentAlias",
        "bedrock:DeleteAgentAlias",
        "bedrock:ListAgentActionGroups",
        "bedrock:GetAgentActionGroup",
        "bedrock:CreateAgentActionGroup",
        "bedrock:UpdateAgentActionGroup",
        "bedrock:DeleteAgentActionGroup",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:AssociateAgentKnowledgeBase",
        "bedrock:DisassociateAgentKnowledgeBase",
        "bedrock:UpdateAgentKnowledgeBase",
        "bedrock:CreateKnowledgeBase",
        "bedrock:UpdateKnowledgeBase",
        "bedrock:DeleteKnowledgeBase",
        "bedrock:ListDataSources",
        "bedrock:GetDataSource",
        "bedrock:CreateDataSource",
        "bedrock:UpdateDataSource",
        "bedrock:DeleteDataSource",
        "bedrock:ListIngestionJobs",
        "bedrock:GetIngestionJob",
        "bedrock:StartIngestionJob",
        "bedrock:StopIngestionJob",
        "bedrock:CreateGuardrail",
        "bedrock:UpdateGuardrail",
        "bedrock:DeleteGuardrail",
        "bedrock:CreateGuardrailVersion",
        "bedrock:CreatePrompt",
        "bedrock:UpdatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:CreateFlow",
        "bedrock:UpdateFlow",
        "bedrock:PrepareFlow",
```

```
        "bedrock:DeleteFlow",
        "bedrock:ListFlowAliases",
        "bedrock:GetFlowAlias",
        "bedrock:CreateFlowAlias",
        "bedrock:UpdateFlowAlias",
        "bedrock:DeleteFlowAlias",
        "bedrock:ListFlowVersions",
        "bedrock:GetFlowVersion",
        "bedrock:CreateFlowVersion",
        "bedrock:DeleteFlowVersion",
        "bedrock:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagBR",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : [
        "arn:aws:bedrock:*:*:agent-alias/*/TSTALIASID",
        "arn:aws:bedrock:*:*:flow/*/alias/TSTALIASID"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngBRJobs",
      "Effect" : "Allow",
      "Action" : "bedrock:BatchDeleteEvaluationJob",
      "Resource" : "*",
```

```
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BRLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:InvokeFunction",
        "lambda:DeleteFunction",
        "lambda:UpdateFunctionCode",
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration",
        "lambda:ListVersionsByFunction",
        "lambda:PublishVersion",
        "lambda:GetPolicy",
        "lambda:AddPermission",
        "lambda:TagResource"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngBRLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:ListTags",
        "lambda:RemovePermission"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRClusterMng",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ModifyInstanceFleet",
        "elasticmapreduce:RunJobFlow",
        "elasticmapreduce:SetTerminationProtection",
        "elasticmapreduce:TerminateJobFlows",
        "elasticmapreduce:DescribeCluster"
      ],
      "Resource" : "arn:aws:elasticmapreduce:*:*:cluster/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AirflowEnv",
      "Effect" : "Allow",
      "Action" : [
        "airflow:CreateEnvironment",
        "airflow:UpdateEnvironment",
        "airflow:DeleteEnvironment",
        "airflow:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "AirflowS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "VpcCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "ENICreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "KmsCreate",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "airflow.*.amazonaws.com",
            "neptune-graph.*.amazonaws.com",
            "s3vectors.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KmsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QueryRoleMng",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        }
      }
    },
    {
      "Sid" : "QueryRoleCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
    },
    {
      "Sid" : "QueryRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioQueryExecutionRolePolicy"
          ]
        }
      }
    },
    {
      "Sid" : "TagQueryRole",
      "Effect" : "Allow",
      "Action" : "iam:TagRole",
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "CreatedForUseWithSageMakerStudio",
            "SageMakerStudioQueryExecutionRole"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "ListQueryPolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
    },
    {
      "Sid" : "EMRCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EmrRoleCleanup",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListInstanceProfilesForRole",
        "iam:DeleteRolePolicy",
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/datazone_emr_*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EmrInstanceCleanup",
      "Effect" : "Allow",
      "Action" : [
        "iam:RemoveRoleFromInstanceProfile",
```

```
        "iam:DeleteInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/
datazone_emr_ec2_instance_profile_*"
    },
    {
      "Sid" : "Scheduler",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListTagsForResource",
        "scheduler:GetScheduleGroup"
      ],
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ScheduleGroup",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:DeleteScheduleGroup",
        "scheduler:UntagResource"
      ],
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CreateSchedule",
      "Effect" : "Allow",
      "Action" : "scheduler:CreateScheduleGroup",
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "AmazonDataZone*"
```

```
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagSchedule",
      "Effect" : "Allow",
      "Action" : "scheduler:TagResource",
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "AmazonDataZone*"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DeleteSchedule",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:DeleteSchedule"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule/SageMakerUnifiedStudio-*-*/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "MngQSFolder",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSource",
        "quicksight:CreateFolder",
        "quicksight:CreateFolderMembership",
        "quicksight:CreateVPCConnection",
        "quicksight:DeleteDataSource",
        "quicksight:DeleteFolder",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeFolderPermissions",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DeleteVPCConnection",
        "quicksight:ListFolderMembers",
        "quicksight:ListTagsForResource",
        "quicksight:UpdateDataSource",
        "quicksight:UpdateDataSourcePermissions",
        "quicksight:UpdateFolder",
        "quicksight:UpdateFolderPermissions",
        "quicksight:UpdateVPCConnection"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QuickSightResources",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
```

```
        "quicksight:DescribeFolder",
        "quicksight:DescribeGroup",
        "quicksight:DescribeGroupMembership",
        "quicksight:DescribeUser",
        "quicksight:DescribeVPCConnection",
        "quicksight:ListTagsForResource",
        "quicksight:UpdateDashboardPermissions"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagQS",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:TagResource"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PassRoleForQS",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/service-role/AmazonSageMakerQuickSightVPC",
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "quicksight.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PutRule",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/Managed.SageMaker*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.quicksight",
            "aws.codecommit"
          ]
        },
        "Null" : {
          "events:detail-type" : "false",
          "events:source" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "events:ManagedBy" : "datazone.amazonaws.com",
          "events:detail-type" : [
            "AWS Service Event via CloudTrail",
            "CodeCommit Repository State Change"
          ]
        }
      }
    },
    {
      "Sid" : "MngEventRules",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutTargets",
        "events:RemoveTargets"
```

```
      ],
      "Resource" : "arn:aws:events:*:*:rule/Managed.SageMaker*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "events:ManagedBy" : "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "RssAdmin",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3AGPerm",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccessGrantsInstance",
        "s3:CreateAccessGrantsInstance"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ResourceTagsUnTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:UntagResource",
```

```
        "neptune-graph:UntagResource",
        "quicksight:UntagResource",
        "glue:UntagResource",
        "airflow:UntagResource",
        "secretsmanager:UntagResource",
        "lambda:UntagResource",
        "emr-serverless:UntagResource",
        "elasticmapreduce:RemoveTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SSOMng",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication",
        "sso:DeleteApplication",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:ListInstances",
        "sso:PutApplicationAccessScope",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationGrant",
        "sso:PutApplicationSessionConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "elasticmapreduce.amazonaws.com",
            "emr-containers.amazonaws.com",
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "ops.emr-serverless.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "EmrContainersMng",
      "Effect" : "Allow",
      "Action" : [
        "emr-containers:CreateManagedEndpoint",
        "emr-containers:CreateSecurityConfiguration",
        "emr-containers:CreateVirtualCluster",
        "emr-containers:DeleteManagedEndpoint",
        "emr-containers:DeleteSecurityConfiguration",
        "emr-containers:DeleteVirtualCluster",
        "emr-containers:DescribeSecurityConfiguration",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "MngViaEmrContainers",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeNetworkInterfaces",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "eks:AssociateAccessPolicy",
        "eks:CreateAccessEntry",
        "eks:DisassociateAccessPolicy",
        "eks:DeleteAccessEntry",
        "eks:DescribeAccessEntry",
        "eks:ListAssociatedAccessPolicies"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "emr-containers.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioProjectRoleMachineLearningPolicy

Deskripsi: Amazon SageMaker Studio membuat peran IAM bagi pengguna proyek untuk melakukan analitik data, kecerdasan buatan, dan tindakan pembelajaran mesin, dan menggunakan kebijakan ini saat membuat peran ini untuk menentukan izin yang terkait SageMaker.

`SageMakerStudioProjectRoleMachineLearningPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioProjectRoleMachineLearningPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 November 2024, 21:55 UTC
- Waktu teredit: 14 September 2026, 20:37 UTC

- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectRoleMachineLearningPolicy`

Versi kebijakan

Versi kebijakan: v44 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowManageSageMakerEniOnVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:Vpc" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}"
        },
        "StringEquals" : {
          "aws:CalledViaLast" : [
            "sagemaker.amazonaws.com",
            "airflow.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManageSageMakerTrainingEniOnVpc",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:Vpc" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}"
        }
      }
    },
    {
      "Sid" : "AllowManageSageMakerEni",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "sagemaker.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSageMakerCreateVpcEndpointOnVpcId",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}",
      "Condition" : {
        "StringEquals" : {
          "ec2:VpcID" : "${aws:PrincipalTag/VpcId}"
        },
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "sagemaker.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSageMakerCreateVpcEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "sagemaker.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSageMakerDescribeVPCResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "glue:ListSessions",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeDhcpOptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSageMakerLogAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
    },
    {
      "Sid" : "SageMakerMlflowPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:UpdateMlflowTrackingServer",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker-mlflow:*"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerMlflowServerlessPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateMlflowApp",
        "sagemaker:CreatePresignedMlflowAppUrl",
        "sagemaker:DeleteMlflowApp",
        "sagemaker:DescribeMlflowApp",
        "sagemaker:UpdateMlflowApp",
        "sagemaker:CallMlflowAppApi"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-app/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
```

```
    },
    {
      "Sid" : "SageMakerBYOFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerBYOIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeImageVersion",
        "sagemaker:ListImageVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerStudioAppDescribeImageActionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeImage"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:image/*"
    },
    {
      "Sid" : "SageMakerPipelinesSTSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerLogPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
```

```
    },
    {
      "Sid" : "SageMakerCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateAutoMLJobV2",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateInferenceComponent",
        "sagemaker:CreatePipeline",
        "sagemaker:CreateInferenceRecommendationsJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerInferencePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:StopTrainingJob",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchPutMetrics",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
```

```
        "sagemaker:UpdateInferenceComponentRuntimeConfig",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteInferenceComponent",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:InvokeEndpointWithResponseStream",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeOptimizationJob",
        "sagemaker:DescribeEndpoint"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerUpdateInferenceComponentRuntimeConfigAutoscalingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:UpdateInferenceComponentRuntimeConfig"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "application-autoscaling.amazonaws.com",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerDescribeUpdateDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeInferenceRecommendationsJob",
```

```
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:UpdatePipeline",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DeletePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopPipelineExecution",
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
        "sagemaker:RetryPipelineExecution",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeTrainingJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerLineageSpecialPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateContext",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAction",
        "sagemaker:AddAssociation",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteArtifact"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerModelRegistryLineageSpecialPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:QueryLineage",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeContext"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:GetSearchSuggestions",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListEndpoints",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListModels",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListHubs",
        "sagemaker:ListPipelines",
        "sagemaker:ListContexts",
        "sagemaker:ListMlflowApps",
```

```
        "sagemaker:ListFeatureGroups",
        "scheduler:ListSchedules"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerSearchPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:Search"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "sagemaker:SearchVisibilityCondition/Tags.AmazonDataZoneProject/
EqualsIfExists" : "${aws:PrincipalTag/AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerListPermissionsTagRestricted",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListHubContents",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
```

```
    },
    {
      "Sid" : "SageMakerPublicHubReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeHub",
        "sagemaker:DescribeHubContent",
        "sagemaker:ListHubContents"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub",
        "arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerECRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*"
    },
    {
      "Sid" : "SageMakerECRGetAuthorizationTokenPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupGetPermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupListPermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupWritePermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:collection" : "false"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupDeletePermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:DeleteGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:collection" : "false"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerMLFlowModelRegistrationPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeModelPackageGroup"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:model-package-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioCreatePresignedDomainUrlForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*/${aws:PrincipalTag/
datazone:userId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
```

```
    },
    {
      "Sid" : "SageMakerStudioCreatePresignedDomainUrlForTaggedUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAppListActionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListApps",
        "sagemaker:ListDomains",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListSpaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerStudioAppDescribeDomainActionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAppDescribeJupyterLabAppActionPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/*/codeeditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/CodeEditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/jupyterlab/*",
        "arn:aws:sagemaker:*:*:app/*/*/JupyterLab/*"
      ]
    },
    {
      "Sid" : "SageMakerStudioAppDescribeUserProfileActionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*/${aws:PrincipalTag/
datazone:userId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAppDescribeTaggedUserProfilePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SMStudioAppDescribeSpaceActionPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:DescribeSpace"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*",
            "sagemaker*",
            "sm-jumpstart*",
            "endpoint-has-jumpstart-model"
          ]
        },
        "ForAllValues:StringNotLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "sagemaker:shared-with:*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAllowCreatingDeletingOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteUserProfile",
        "sagemaker:UpdateUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*/${aws:PrincipalTag/
datazone:userId}",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAllowCreatingDeletingTaggedOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteUserProfile",
        "sagemaker:UpdateUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/*/
${aws:PrincipalTag/datazone:userId}"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceToOwnerUser",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceAppsToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/*/codeeditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/CodeEditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/jupyterlab/*",
        "arn:aws:sagemaker:*:*:app/*/*/JupyterLab/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/*/
${aws:PrincipalTag/datazone:userId}"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
```

```
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceAppsToOwnerUser",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/*/CodeEditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/codeeditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/jupyterlab/*",
        "arn:aws:sagemaker:*:*:app/*/*/JupyterLab/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStartSessionForSpaceRemoteConnection",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:StartSession"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
```

```
    },
    {
      "Sid" : "PublishSagemakerMetric",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : "/aws/sagemaker/*"
        }
      }
    },
    {
      "Sid" : "ManageSageMakerEndpointsAutoscalingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MutateSageMakerEndpointsAutoscalingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:TargetTracking*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "application-autoscaling.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SSMPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
    },
    {
      "Sid" : "SageMakerJumpstartS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::jumpstart-cache-prod-*/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerCrossAccountPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:ListModelPackages",
        "sagemaker:CreateModel"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerListTagsRestrictionOnSharedResources",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerFeatureStorePermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*Feature*",
        "sagemaker:*Record"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerAutoScalingPermissionsWithserviceNamespace",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "arn:aws:application-autoscaling:*:*:scalable-target/*",
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "sagemaker",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "SageMakerAutoScalingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions"
      ],
      "Resource" : "arn:aws:application-autoscaling:*:*:scalable-target/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerSLRForAutoScalingPermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "sagemaker.*.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "S3AGObjectRead",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnEquals" : {
          "s3:AccessGrantsInstanceArn" : [
            "arn:aws:s3:*:*:access-grants/default"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3AGObjectWrite",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnEquals" : {
          "s3:AccessGrantsInstanceArn" : [
            "arn:aws:s3:*:*:access-grants/default"
```

```
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3AGBucketLevelReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "ArnEquals" : {
          "s3:AccessGrantsInstanceArn" : [
            "arn:aws:s3:*:*:access-grants/default"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3AGKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:s3:arn"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "S3AGLocationManagement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateAccessGrantsLocation",
        "s3:DeleteAccessGrantsLocation",
        "s3:GetAccessGrantsLocation"
      ],
      "Resource" : [
        "arn:aws:s3:*:*:access-grants/default/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:accessGrantsLocationScope" : "s3://${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/"
        }
      }
    },
    {
      "Sid" : "S3AGPermissionManagement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateAccessGrant",
        "s3:DeleteAccessGrant"
      ],
      "Resource" : [
        "arn:aws:s3:*:*:access-grants/default/location/*",
        "arn:aws:s3:*:*:access-grants/default/grant/*"
      ],
      "Condition" : {
        "StringLike" : {
          "s3:accessGrantScope" : "s3://${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*"
        }
      }
    },
    {
      "Sid" : "CrossAccountS3AGResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : [
            "s3:AccessGrants"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountS3AGResourceSharingPolicyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutAccessGrantsInstanceResourcePolicy"
      ],
      "Resource" : "arn:aws:s3:*:*:access-grants/default",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3AGTaggingPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:TagResource",
        "s3:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:s3:*:*:access-grants/default/location/*",
        "arn:aws:s3:*:*:access-grants/default/grant/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ConsumerS3AGPermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccessGrantsInstanceForPrefix",
        "s3:GetDataAccess",
        "s3:ListCallerAccessGrants",
        "ram:GetResourceShareInvitations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MLAccountDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "airflow-serverless:ListWorkflow*",
        "airflow-serverless:ListTask*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowServerlessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "airflow-serverless:CreateWorkflow",
        "airflow-serverless:DeleteWorkflow",
        "airflow-serverless:GetTaskInstance",
        "airflow-serverless:GetWorkflow",
        "airflow-serverless:GetWorkflowRun",
        "airflow-serverless:ListTagsForResource",
        "airflow-serverless:StartWorkflowRun",
        "airflow-serverless:StopWorkflowRun",
        "airflow-serverless:TagResource",
        "airflow-serverless:UntagResource",
        "airflow-serverless:UpdateWorkflow"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AirflowCloudwatchLogsActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/mwaa-serverless/${aws:PrincipalTag/
AmazonDataZoneDomain}-${aws:PrincipalTag/AmazonDataZoneProject}/*"
      ]
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless"
      ]
    },
    {
      "Sid" : "DataZoneUserPermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:GenerateCode",
        "datazone:CreateAsset*",
        "datazone:List*",
        "datazone:Search*",
        "datazone:*Message*",
        "datazone:*Conversation*",
        "datazone:*Cell*",
        "datazone:*Notebook*",
        "datazone:*Compute*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaSession",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetSessionEndpoint",
        "athena:GetResourceDashboard",
        "athena:TagResource"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SQLWorkBenchMLActionsWithResourceType",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:GetConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioProjectUserRolePermissionsBoundary

Deskripsi: SageMaker Amazon membuat peran IAM bagi pengguna Proyek untuk melakukan analitik data, kecerdasan buatan, dan tindakan pembelajaran mesin, dan menggunakan kebijakan ini saat membuat peran ini untuk menentukan batas izin mereka.

`SageMakerStudioProjectUserRolePermissionsBoundary`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioProjectUserRolePermissionsBoundary` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 November 2024, 21:57 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePermissionsBoundary`

Versi kebijakan

Versi kebijakan: v19 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DenyAllNonMatchingProjectTag",
      "Effect" : "Deny",
      "Action" : "*",
      "NotResource" : [
        "arn:*:sagemaker:*:*:model-package-group/*",
        "arn:*:sagemaker:*:*:model-package/*",
        "arn:*:glue:*:*:catalog/*",
        "arn:*:glue:*:*:database/*"
      ],
      "Condition" : {
```

```
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:PrincipalTag/AmazonDataZoneProject" : "false",
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true"
        },
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AmazonQChatPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataLakeS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SameAccountKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
```

```
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "emr-serverless.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "redshift-serverless.*.amazonaws.com",
            "bedrock.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com",
            "ec2.*.amazonaws.com",
            "codecommit.*.amazonaws.com",
            "glue.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGenerateDataKeyForEmrEbsEncryption",
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SameAccountKMSManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:RevokeGrant",
        "kms:DescribeKey"
```

```
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "emr-serverless.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "bedrock.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com",
            "codecommit.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CrossAccountS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
```

```
        "s3:ListMultipartUploadParts",
        "s3:ListBucket",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CrossAccountKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "CrossAccountKMSManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListGrants",
```

```
        "kms:GetPublicKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DataZoneKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "datazone.*.amazonaws.com"
          ]
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "DataZoneDescribeKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "datazone.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}",
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
          ]
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
```

```
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListDomainBucketFromAthenaFederatedCatalog",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}"
      ],
      "Condition" : {
        "ArnEquals" : {
          "lambda:SourceFunctionArn" :
 "arn:aws:lambda:*:*:function:athenafederatedcatalog_*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
```

```
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessCertificateS3LocationPermissions",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/certificate_location/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagS3ObjectPermissionsForBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : "s3:PutObjectTagging",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
genAI/assets/evaluations/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "s3:RequestObjectTag/BasicValidationStatus" : [
```

```
            "valid",
            "invalid"
          ],
          "s3:RequestObjectTag/ContainsReferenceResponseForAllPrompts" : [
            "true",
            "false"
          ]
        },
        "ForAllValues:StringEquals" : {
          "s3:RequestObjectTagKeys" : [
            "BasicValidationStatus",
            "ContainsReferenceResponseForAllPrompts"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchDescribeLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:StartQuery",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/*",
        "arn:aws:logs:*:*:log-group:airflow*",
        "arn:aws:logs:*:*:log-group:datazone*"
      ]
```

```
    },
    {
      "Sid" : "CloudWatchStopQuery",
      "Effect" : "Allow",
      "Action" : [
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaPermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "athena:TerminateSession",
        "athena:CreatePreparedStatement",
        "athena:StopCalculationExecution",
        "athena:StartQueryExecution",
        "athena:UpdatePreparedStatement",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:UpdateNotebook",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:UpdateNotebookMetadata",
```

```
        "athena:DeleteNamedQuery",
        "athena:GetCalculationExecution",
        "athena:GetCalculationExecutionCode",
        "athena:GetCalculationExecutionStatus",
        "athena:GetNamedQuery",
        "athena:GetNotebookMetadata",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetSession",
        "athena:GetSessionStatus",
        "athena:GetWorkGroup",
        "athena:UpdateNamedQuery",
        "athena:CreateNamedQuery",
        "athena:ExportNotebook",
        "athena:StopQueryExecution",
        "athena:StartCalculationExecution",
        "athena:StartSession",
        "athena:CreatePresignedNotebookUrl",
        "athena:CreateNotebook",
        "athena:ImportNotebook",
        "athena:ListQueryExecutions",
        "athena:ListTagsForResource",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DataZonePermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:CreateConnection",
        "datazone:DeleteConnection",
        "datazone:GetConnection",
        "datazone:GetDomain",
        "datazone:GetDomainExecutionRoleCredentials",
```

```
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetProject",
        "datazone:GetUserProfile",
        "datazone:ListConnections",
        "datazone:ListEnvironments",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListProjects",
        "datazone:UpdateConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueDatalakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:GetCatalogImportStatus",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:ListTableOptimizerRuns",
```

```
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:GetCatalogs",
        "glue:GetCatalog",
        "glue:UpdateCatalog"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueCrawlerPermissions",
      "Effect" : "Allow",
      "Action" : "glue:ListCrawls",
      "Resource" : "arn:aws:glue:*:*:crawler/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueGlobalTempDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/global_temp",
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "GlueCatalogDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
```

```
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "GlueUnrestrictedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UseGlueStudio",
        "glue:ListSessions",
        "glue:StartCompletion",
        "glue:GetCompletion",
        "glue:GetGeneratedCode",
        "glue:GetTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GluePermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:PassConnection",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:CancelStatement",
        "glue:ListStatements",
        "glue:TagResource",
        "glue:UntagResource",
        "glue:DeleteSession",
        "glue:RunStatement",
        "glue:StopSession",
        "glue:GetDashboardUrl",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
```

```
        "glue:PutWorkflowRunProperties",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:ResumeWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:StartJobRun",
        "glue:CancelDataQualityRuleRecommendationRun",
        "glue:CancelDataQualityRulesetEvaluationRun",
        "glue:DeleteDataQualityRuleset",
        "glue:GetDataQualityModel",
        "glue:GetDataQualityModelResult",
        "glue:GetDataQualityResult",
        "glue:GetDataQualityRuleRecommendationRun",
        "glue:GetDataQualityRuleset",
        "glue:GetDataQualityRulesetEvaluationRun",
        "glue:ListDataQualityResults",
        "glue:ListDataQualityRuleRecommendationRuns",
        "glue:ListDataQualityRulesetEvaluationRuns",
        "glue:ListDataQualityRulesets",
        "glue:PublishDataQuality",
        "glue:PutDataQualityProfileAnnotation",
        "glue:PutDataQualityStatisticAnnotation",
        "glue:StartDataQualityRuleRecommendationRun",
        "glue:StartDataQualityRulesetEvaluationRun",
        "glue:UpdateDataQualityRuleset"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "GlueCreateAndTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession",
```

```
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateDataQualityRuleset",
        "glue:CreateWorkflow",
        "glue:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IAMListRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "sagemaker.amazonaws.com",
            "ec2.amazonaws.com",
            "emr-serverless.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "RedshiftDataActionsIAMSessionRestriction",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RedshiftUnrestrictedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusters",
        "sqlworkbench:PutTab",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:ListTabs",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource",
        "sqlworkbench:PassAccountSettings",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:CreateConnection",
```

```
        "sqlworkbench:PutQCustomContext",
        "sqlworkbench:GetQCustomContext",
        "sqlworkbench:DeleteQCustomContext",
        "sqlworkbench:GetQSqlRecommendations",
        "sqlworkbench:GetQSqlPromptQuotas",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftPermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListTagsForResource",
        "redshift:DescribeTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AllowAccessExistingRedshiftCompute",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetCredentials",
        "redshift:DescribeTags",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftDataActionsForManagedWorkgroup",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:GetStagingBucketLocation",
        "redshift-serverless:GetManagedWorkgroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "redshift-data:glue-catalog-arn" : "arn:aws:glue:*:*:catalog/*"
        }
      }
    },
    {
      "Sid" : "RedshifServerlessCredentialsForManagedWorkgroup",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "arn:aws:redshift-serverless:*:*:workgroup/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "redshift-data.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftExistingComputeConnectToCatalog",
      "Effect" : "Allow",
      "Action" : [
```

```
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "arn:aws:redshift:*:*:dbname:*/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "GenerativeAIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockAppInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockModelInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:*-model/*"
      ],
      "Condition" : {
        "Null" : {
```

```
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "ManageNetworkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateTags",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListImageVersions",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListContexts",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListEndpoints",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListModels",
```

```
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListHubContents",
        "sagemaker:ListHubs",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListApps",
        "sagemaker:ListDomains",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListSpaces",
        "sagemaker:ListTags",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeOptimizationJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeSpace",
```

```
        "sagemaker:AddTags",
        "sagemaker:AddAssociation",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteUserProfile",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:DeleteApp",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateSpace",
        "sagemaker:CreateApp",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateAutoMLJobV2",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreatePipeline",
        "sagemaker:CreateContext",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAction",
        "sagemaker:CreateInferenceComponent",
        "sagemaker:UpdateInferenceComponentRuntimeConfig",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchPutMetrics",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
```

```
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteInferenceComponent",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:InvokeEndpointWithResponseStream",
        "sagemaker:QueryLineage",
        "sagemaker:UpdatePipeline",
        "sagemaker:DeletePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopPipelineExecution",
        "sagemaker:RetryPipelineExecution",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:Search",
        "sagemaker:UpdateMlflowTrackingServer",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker:ListPartnerApps",
        "sagemaker:CreatePartnerAppPresignedUrl",
        "sagemaker:DescribePartnerApp",
        "sagemaker:CallPartnerAppApi",
        "sagemaker-mlflow:AccessUI",
        "sagemaker-mlflow:CreateExperiment",
        "sagemaker-mlflow:SearchExperiments",
        "sagemaker-mlflow:GetExperiment",
        "sagemaker-mlflow:GetExperimentByName",
        "sagemaker-mlflow:DeleteExperiment",
        "sagemaker-mlflow:RestoreExperiment",
        "sagemaker-mlflow:UpdateExperiment",
        "sagemaker-mlflow:CreateRun",
        "sagemaker-mlflow:DeleteRun",
        "sagemaker-mlflow:RestoreRun",
        "sagemaker-mlflow:GetRun",
        "sagemaker-mlflow:LogMetric",
        "sagemaker-mlflow:LogBatch",
```

```
        "sagemaker-mlflow:LogModel",
        "sagemaker-mlflow:LogInputs",
        "sagemaker-mlflow:SetExperimentTag",
        "sagemaker-mlflow:SetTag",
        "sagemaker-mlflow:DeleteTag",
        "sagemaker-mlflow:LogParam",
        "sagemaker-mlflow:GetMetricHistory",
        "sagemaker-mlflow:SearchRuns",
        "sagemaker-mlflow:ListArtifacts",
        "sagemaker-mlflow:UpdateRun",
        "sagemaker-mlflow:CreateRegisteredModel",
        "sagemaker-mlflow:GetRegisteredModel",
        "sagemaker-mlflow:RenameRegisteredModel",
        "sagemaker-mlflow:UpdateRegisteredModel",
        "sagemaker-mlflow:DeleteRegisteredModel",
        "sagemaker-mlflow:GetLatestModelVersions",
        "sagemaker-mlflow:CreateModelVersion",
        "sagemaker-mlflow:GetModelVersion",
        "sagemaker-mlflow:UpdateModelVersion",
        "sagemaker-mlflow:DeleteModelVersion",
        "sagemaker-mlflow:SearchModelVersions",
        "sagemaker-mlflow:GetDownloadURIForModelVersionArtifacts",
        "sagemaker-mlflow:TransitionModelVersionStage",
        "sagemaker-mlflow:SearchRegisteredModels",
        "sagemaker-mlflow:SetRegisteredModelTag",
        "sagemaker-mlflow:DeleteRegisteredModelTag",
        "sagemaker-mlflow:DeleteModelVersionTag",
        "sagemaker-mlflow:DeleteRegisteredModelAlias",
        "sagemaker-mlflow:SetRegisteredModelAlias",
        "sagemaker-mlflow:GetModelVersionByAlias",
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:DescribeImages",
        "elasticfilesystem:DescribeMountTargets",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath",
        "ec2:DescribeInstanceTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerSLRForAutoScalingPermissions",
```

```
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ComputePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
        "sts:GetCallerIdentity",
        "sts:TagSession",
        "emr-serverless:GetApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRunAttempts",
        "emr-serverless:ListJobRuns",
        "emr-serverless:StartApplication",
        "emr-serverless:StartJobRun",
        "emr-serverless:StopApplication",
        "emr-serverless:AccessInteractiveEndpoints",
        "emr-serverless:AccessLivyEndpoints",
        "elasticmapreduce:ListReleaseLabels",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:CreatePersistentAppUI",
        "elasticmapreduce:DescribePersistentAppUI",
        "elasticmapreduce:GetPersistentAppUIPresignedURL",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sts:AssumeRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "SetSourceIdentityForAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "AllowListSecrets",
      "Effect" : "Allow",
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*"
    },
    {
      "Sid" : "ComputePermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetCredentials",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
```

```
        "redshift-data:ListTables",
        "elasticmapreduce:GetClusterSessionCredentials",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetOnClusterAppUIPresignedURL",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:TerminateJobFlows",
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DataLakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeCommitPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:BatchGetCommits",
        "codecommit:BatchGetPullRequests",
        "codecommit:BatchGetRepositories",
        "codecommit:BatchDescribeMergeConflicts",
        "codecommit:CreateBranch",
        "codecommit:CreateCommit",
        "codecommit:CreatePullRequest",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:DescribeMergeConflicts",
        "codecommit:DescribePullRequestEvents",
        "codecommit:GetBlob",
        "codecommit:GetBranch",
```

```
        "codecommit:GetComment",
        "codecommit:GetCommentReactions",
        "codecommit:GetCommentsForComparedCommit",
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommit",
        "codecommit:GetCommitHistory",
        "codecommit:GetCommitsFromMergeBase",
        "codecommit:GetDifferences",
        "codecommit:GetFile",
        "codecommit:GetFolder",
        "codecommit:GetMergeCommit",
        "codecommit:GetMergeConflicts",
        "codecommit:GetMergeOptions",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetPullRequest",
        "codecommit:GetPullRequestApprovalStates",
        "codecommit:GetPullRequestOverrideState",
        "codecommit:GetReferences",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:GetTree",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:ListAssociatedApprovalRuleTemplatesForRepository",
        "codecommit:ListBranches",
        "codecommit:ListFileCommitHistory",
        "codecommit:ListPullRequests",
        "codecommit:ListTagsForResource",
        "codecommit:MergeBranchesByFastForward",
        "codecommit:MergeBranchesBySquash",
        "codecommit:MergeBranchesByThreeWay",
        "codecommit:MergePullRequestByFastForward",
        "codecommit:MergePullRequestBySquash",
        "codecommit:MergePullRequestByThreeWay",
        "codecommit:UpdateComment",
        "codecommit:UpdateDefaultBranch",
        "codecommit:UpdatePullRequestApprovalRuleContent",
        "codecommit:UpdatePullRequestApprovalState",
        "codecommit:UpdatePullRequestDescription",
        "codecommit:UpdatePullRequestStatus",
        "codecommit:UpdatePullRequestTitle",
        "codecommit:UpdateRepositoryDescription",
        "codecommit:PostCommentForComparedCommit",
```

```
        "codecommit:PostCommentForPullRequest",
        "codecommit:PostCommentReply",
        "codecommit:PutCommentReaction",
        "codecommit:PutFile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EMRServicePermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScheduledAction",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreatePlacementGroup",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeletePlacementGroup",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
```

```
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcAttribute",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModelRegistryResourceGroupGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModelRegistryResourceGroupMutatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:collection" : "false"
        }
      }
    },
    {
      "Sid" : "ModelRegistryBedRockPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessAossCollectionsForBedrock",
      "Effect" : "Allow",
```

```
      "Action" : "aoss:APIAccessAll",
      "Resource" : "*"
    },
    {
      "Sid" : "AccessBedrockResources",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:InvokeAgent",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:Retrieve",
        "bedrock:StartIngestionJob",
        "bedrock:GetIngestionJob",
        "bedrock:ListIngestionJobs",
        "bedrock:ApplyGuardrail",
        "bedrock:ListPrompts",
        "bedrock:GetPrompt",
        "bedrock:CreatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:InvokeFlow",
        "bedrock:GetEvaluationJob",
        "bedrock:CreateEvaluationJob",
        "bedrock:StopEvaluationJob",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:ListTagsForResource",
        "bedrock:CreateAgentAlias",
        "bedrock:ListAgentAliases",
        "bedrock:GetAgentVersion",
        "bedrock:ListAgentVersions",
        "bedrock:DeleteAgentVersion",
        "bedrock:DeleteAgentAlias",
        "bedrock:GetAgentAlias",
        "bedrock:UpdateAgentAlias"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
```

```
      }
    },
    {
      "Sid" : "CreateEvaluationJobForFoundationModel",
      "Effect" : "Allow",
      "Action" : "bedrock:CreateEvaluationJob",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*"
      ]
    },
    {
      "Sid" : "InvokeBedrockInlineAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeInlineAgent",
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockRetrieveAndGeneratePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
      "Sid" : "ListBedrockEvaluationJobPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ListEvaluationJobs",
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrockEvaluationRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "TagBedrockResourcePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockKnowledgeBaseDataIngestionKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "kms:ViaService" : "true",
          "kms:EncryptionContext:aws:bedrock:arn" : "false"
        }
      }
    },
    {
      "Sid" : "AccessSecretPermissionsForBedrockApp",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "InvokeFunctionPermissionsForBedrockApp",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GetDataZoneEnvironmentCfnStackPermissionsForBedrockAppExport",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplate",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/DataZone-Env-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "MWAAPermissions",
      "Effect" : "Allow",
      "Action" : [
        "airflow:ListEnvironments",
        "airflow:GetEnvironment",
        "airflow:UpdateEnvironment",
        "airflow:CreateWebLoginToken",
        "airflow:InvokeRestApi"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AirflowS3GetAccountPublicAccessBlock",
      "Effect" : "Allow",
      "Action" : "s3:GetAccountPublicAccessBlock",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}"
    },
    {
      "Sid" : "SQSPermissionsForMWAA",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage"
      ],
      "Resource" : "arn:aws:sqs:*:*:airflow-celery-*"
    },
    {
      "Sid" : "FederatedDataConnectionGlueSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GlueConnectionAccessForFederatedDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListConnectionTypes",
        "glue:DescribeConnectionType"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueEntitiesAccessForFederatedDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListEntities",
        "glue:DescribeEntity",
        "glue:GetEntityRecords"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretAccessForForUseWithAllDataZoneProjectsSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "AccessForDynamoDbConnections",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "InvokeFunctionPermissionsForAthenaCatalogLambda",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceTag/federated_athena_datacatalog" : "true"
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketForQueryExecutionRolePermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3PermissionsForAthenaCatalog",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::redshift-staging-bucket-*/*",
        "arn:aws:s3:::redshift-staging-bucket-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "GetS3ObjectForQueryExecutionRolePermissions",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*/dzd_*/*/dev/sys/athena/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetGlueUserDefinedFuncLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GetGlueUserDefinedFuncPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:userDefinedFunction/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "NotDeniedOperations",
      "Effect" : "Deny",
      "NotAction" : [
        "airflow:CreateWebLoginToken",
        "airflow:GetEnvironment",
        "airflow:InvokeRestApi",
        "airflow:ListEnvironments",
        "airflow:UpdateEnvironment",
        "aoss:APIAccessAll",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetCalculationExecution",
        "athena:GetCalculationExecutionCode",
        "athena:GetCalculationExecutionStatus",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetNotebookMetadata",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
```

```
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetSession",
        "athena:GetSessionStatus",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "bedrock:ApplyGuardrail",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:CreateAgentAlias",
        "bedrock:CreateEvaluationJob",
        "bedrock:CreatePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:DeleteAgentAlias",
        "bedrock:DeleteAgentVersion",
        "bedrock:DeletePrompt",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:GetEvaluationJob",
        "bedrock:GetInferenceProfile",
        "bedrock:GetIngestionJob",
        "bedrock:GetPrompt",
```

```
        "bedrock:InvokeAgent",
        "bedrock:InvokeFlow",
        "bedrock:InvokeInlineAgent",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgentVersions",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFoundationModels",
        "bedrock:ListIngestionJobs",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "bedrock:Retrieve",
        "bedrock:RetrieveAndGenerate",
        "bedrock:StartIngestionJob",
        "bedrock:StopEvaluationJob",
        "bedrock:TagResource",
        "bedrock:UpdateAgentAlias",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codecommit:BatchDescribeMergeConflicts",
        "codecommit:BatchGetCommits",
        "codecommit:BatchGetPullRequests",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateBranch",
        "codecommit:CreateCommit",
        "codecommit:CreatePullRequest",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:DescribeMergeConflicts",
        "codecommit:DescribePullRequestEvents",
        "codecommit:GetBlob",
        "codecommit:GetBranch",
        "codecommit:GetComment",
        "codecommit:GetCommentReactions",
        "codecommit:GetCommentsForComparedCommit",
```

```
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommit",
        "codecommit:GetCommitHistory",
        "codecommit:GetCommitsFromMergeBase",
        "codecommit:GetDifferences",
        "codecommit:GetFile",
        "codecommit:GetFolder",
        "codecommit:GetMergeCommit",
        "codecommit:GetMergeConflicts",
        "codecommit:GetMergeOptions",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetPullRequest",
        "codecommit:GetPullRequestApprovalStates",
        "codecommit:GetPullRequestOverrideState",
        "codecommit:GetReferences",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:GetTree",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:ListAssociatedApprovalRuleTemplatesForRepository",
        "codecommit:ListBranches",
        "codecommit:ListFileCommitHistory",
        "codecommit:ListPullRequests",
        "codecommit:ListTagsForResource",
        "codecommit:MergeBranchesByFastForward",
        "codecommit:MergeBranchesBySquash",
        "codecommit:MergeBranchesByThreeWay",
        "codecommit:MergePullRequestByFastForward",
        "codecommit:MergePullRequestBySquash",
        "codecommit:MergePullRequestByThreeWay",
        "codecommit:PostCommentForComparedCommit",
        "codecommit:PostCommentForPullRequest",
        "codecommit:PostCommentReply",
        "codecommit:PutCommentReaction",
        "codecommit:PutFile",
        "codecommit:UpdateComment",
        "codecommit:UpdateDefaultBranch",
        "codecommit:UpdatePullRequestApprovalRuleContent",
        "codecommit:UpdatePullRequestApprovalState",
        "codecommit:UpdatePullRequestDescription",
        "codecommit:UpdatePullRequestStatus",
        "codecommit:UpdatePullRequestTitle",
```

```
        "codecommit:UpdateRepositoryDescription",
        "codewhisperer:GenerateRecommendations",
        "datazone:CreateConnection",
        "datazone:DeleteConnection",
        "datazone:GetConnection",
        "datazone:GetDomain",
        "datazone:GetDomainExecutionRoleCredentials",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetProject",
        "datazone:GetUserProfile",
        "datazone:ListConnections",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironments",
        "datazone:ListProjects",
        "datazone:UpdateConnection",
        "dynamodb:BatchGetItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:Scan",
        "dynamodb:Query",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeEndpoints",
        "dynamodb:DescribeExport",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeImport",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetItem",
        "dynamodb:GetRecords",
        "dynamodb:ListExports",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListImports",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "dynamodb:PutItem",
```

```
        "dynamodb:PartiQLSelect",
        "dynamodb:PartiQLInsert",
        "dynamodb:PartiQLUpdate",
        "dynamodb:PartiQLDelete",
        "dynamodb:UpdateItem",
        "dynamodb:UpdateGlobalTable",
        "dynamodb:UpdateTable",
        "ec2:AttachNetworkInterface",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreatePlacementGroup",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface",
```

```
        "ec2:ModifyInstanceAttribute",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "elasticfilesystem:DescribeMountTargets",
        "elasticmapreduce:CreatePersistentAppUI",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribePersistentAppUI",
        "elasticmapreduce:GetClusterSessionCredentials",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetOnClusterAppUIPresignedURL",
        "elasticmapreduce:GetPersistentAppUIPresignedURL",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListReleaseLabels",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:TerminateJobFlows",
        "emr-serverless:AccessInteractiveEndpoints",
        "emr-serverless:AccessLivyEndpoints",
        "emr-serverless:GetApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRunAttempts",
        "emr-serverless:ListJobRuns",
        "emr-serverless:StartApplication",
        "emr-serverless:StartJobRun",
        "emr-serverless:StopApplication",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
```

```
        "glue:CancelDataQualityRuleRecommendationRun",
        "glue:CancelDataQualityRulesetEvaluationRun",
        "glue:CancelStatement",
        "glue:CreateBlueprint",
        "glue:CreateDatabase",
        "glue:CreateDataQualityRuleset",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateSession",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteDatabase",
        "glue:DeleteDataQualityRuleset",
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteSession",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:DescribeConnectionType",
        "glue:DescribeEntity",
        "glue:GetCatalog",
        "glue:GetCatalogImportStatus",
        "glue:GetCatalogs",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetCompletion",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDashboardUrl",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataQualityModel",
        "glue:GetDataQualityModelResult",
        "glue:GetDataQualityResult",
```

```
        "glue:GetDataQualityRuleRecommendationRun",
        "glue:GetDataQualityRuleset",
        "glue:GetDataQualityRulesetEvaluationRun",
        "glue:GetEntityRecords",
        "glue:GetGeneratedCode",
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
        "glue:GetPartitions",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTags",
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions",
        "glue:ListConnectionTypes",
        "glue:ListCrawls",
        "glue:ListDataQualityResults",
        "glue:ListDataQualityRuleRecommendationRuns",
        "glue:ListDataQualityRulesetEvaluationRuns",
        "glue:ListDataQualityRulesets",
        "glue:ListEntities",
        "glue:ListSessions",
        "glue:ListStatements",
        "glue:ListTableOptimizerRuns",
        "glue:NotifyEvent",
        "glue:PassConnection",
        "glue:PublishDataQuality",
        "glue:PutDataQualityProfileAnnotation",
        "glue:PutDataQualityStatisticAnnotation",
        "glue:PutWorkflowRunProperties",
        "glue:ResumeWorkflowRun",
        "glue:RunStatement",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCompletion",
        "glue:StartDataQualityRuleRecommendationRun",
        "glue:StartDataQualityRulesetEvaluationRun",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopSession",
```

```
        "glue:StopWorkflowRun",
        "glue:TagResource",
        "glue:UntagResource",
        "glue:UpdateBlueprint",
        "glue:UpdateCatalog",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateDataQualityRuleset",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow",
        "glue:UseGlueStudio",
        "iam:CreateServiceLinkedRole",
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole",
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:GetPublicKey",
        "kms:ListAliases",
        "kms:ListGrants",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:RevokeGrant",
        "lakeformation:GetDataAccess",
        "lambda:InvokeFunction",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetLogRecord",
        "logs:GetQueryResults",
        "logs:PutLogEvents",
        "logs:StartQuery",
        "logs:StopQuery",
        "pricing:GetProducts",
```

```
        "q:SendMessage",
        "q:StartConversation",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStagingBucketLocation",
        "redshift-data:GetStatementResult",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListStatements",
        "redshift-data:ListTables",
        "redshift-serverless:GetCredentials",
        "redshift-serverless:GetManagedWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusters",
        "redshift:DescribeTags",
        "redshift:GetClusterCredentialsWithIAM",
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources",
        "resource-groups:Tag",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketLocation",
        "s3:GetEncryptionConfiguration",
        "s3:GetObject*",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:PutObjectTagging",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "sagemaker-mlflow:AccessUI",
```

```
        "sagemaker-mlflow:CreateExperiment",
        "sagemaker-mlflow:CreateModelVersion",
        "sagemaker-mlflow:CreateRegisteredModel",
        "sagemaker-mlflow:CreateRun",
        "sagemaker-mlflow:DeleteExperiment",
        "sagemaker-mlflow:DeleteModelVersion",
        "sagemaker-mlflow:DeleteModelVersionTag",
        "sagemaker-mlflow:DeleteRegisteredModel",
        "sagemaker-mlflow:DeleteRegisteredModelAlias",
        "sagemaker-mlflow:DeleteRegisteredModelTag",
        "sagemaker-mlflow:DeleteRun",
        "sagemaker-mlflow:DeleteTag",
        "sagemaker-mlflow:GetDownloadURIForModelVersionArtifacts",
        "sagemaker-mlflow:GetExperiment",
        "sagemaker-mlflow:GetExperimentByName",
        "sagemaker-mlflow:GetLatestModelVersions",
        "sagemaker-mlflow:GetMetricHistory",
        "sagemaker-mlflow:GetModelVersion",
        "sagemaker-mlflow:GetModelVersionByAlias",
        "sagemaker-mlflow:GetRegisteredModel",
        "sagemaker-mlflow:GetRun",
        "sagemaker-mlflow:ListArtifacts",
        "sagemaker-mlflow:LogBatch",
        "sagemaker-mlflow:LogInputs",
        "sagemaker-mlflow:LogMetric",
        "sagemaker-mlflow:LogModel",
        "sagemaker-mlflow:LogParam",
        "sagemaker-mlflow:RenameRegisteredModel",
        "sagemaker-mlflow:RestoreExperiment",
        "sagemaker-mlflow:RestoreRun",
        "sagemaker-mlflow:SearchExperiments",
        "sagemaker-mlflow:SearchModelVersions",
        "sagemaker-mlflow:SearchRegisteredModels",
        "sagemaker-mlflow:SearchRuns",
        "sagemaker-mlflow:SetExperimentTag",
        "sagemaker-mlflow:SetRegisteredModelAlias",
        "sagemaker-mlflow:SetRegisteredModelTag",
        "sagemaker-mlflow:SetTag",
        "sagemaker-mlflow:TransitionModelVersionStage",
        "sagemaker-mlflow:UpdateExperiment",
        "sagemaker-mlflow:UpdateModelVersion",
        "sagemaker-mlflow:UpdateRegisteredModel",
        "sagemaker-mlflow:UpdateRun",
        "sagemaker:AddAssociation",
```

```
        "sagemaker:AddTags",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CallPartnerAppApi",
        "sagemaker:CreateAction",
        "sagemaker:CreateApp",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateAutoMLJobV2",
        "sagemaker:CreateContext",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateInferenceComponent",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreatePartnerAppPresignedUrl",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateSpace",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteInferenceComponent",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteSpace",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DescribeAction",
```

```
        "sagemaker:DescribeApp",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeOptimizationJob",
        "sagemaker:DescribePartnerApp",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:InvokeEndpointWithResponseStream",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListContexts",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListHubContents",
        "sagemaker:ListHubs",
        "sagemaker:ListHyperParameterTuningJobs",
```

```
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModels",
        "sagemaker:ListPartnerApps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListSpaces",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListUserProfiles",
        "sagemaker:QueryLineage",
        "sagemaker:RetryPipelineExecution",
        "sagemaker:Search",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateInferenceComponentRuntimeConfig",
        "sagemaker:UpdateMlflowTrackingServer",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateSpace",
        "sagemaker:UpdateTrainingJob",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
```

```
        "secretsmanager:ListSecrets",
        "secretsmanager:PutSecretValue",
        "sqlworkbench:CreateConnection",
        "sqlworkbench:DeleteQCustomContext",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource",
        "sqlworkbench:GetQCustomContext",
        "sqlworkbench:GetQSqlPromptQuotas",
        "sqlworkbench:GetQSqlRecommendations",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:ListTabs",
        "sqlworkbench:PassAccountSettings",
        "sqlworkbench:PutQCustomContext",
        "sqlworkbench:PutTab",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath",
        "sts:AssumeRole",
        "sts:GetCallerIdentity",
        "sts:SetSourceIdentity",
        "sts:TagSession",
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioProjectUserRolePolicy

Deskripsi: Amazon SageMaker Studio membuat peran IAM bagi pengguna proyek untuk melakukan analitik data, kecerdasan buatan, dan tindakan pembelajaran mesin, dan menggunakan kebijakan ini saat membuat peran ini untuk menentukan izin.

`SageMakerStudioProjectUserRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioProjectUserRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 November 2024, 21:59 UTC
- Waktu teredit: 27 Agustus 2026, 20:57 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePolicy`

Versi kebijakan

Versi kebijakan: v75 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeCommit",
```

```
      "Effect" : "Allow",
      "Action" : [
        "codecommit:BatchGetCommits",
        "codecommit:BatchGetPullRequests",
        "codecommit:BatchGetRepositories",
        "codecommit:BatchDescribeMergeConflicts",
        "codecommit:CreateBranch",
        "codecommit:CreateCommit",
        "codecommit:CreatePullRequest",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:DescribeMergeConflicts",
        "codecommit:DescribePullRequestEvents",
        "codecommit:GetBlob",
        "codecommit:GetBranch",
        "codecommit:GetComment",
        "codecommit:GetCommentReactions",
        "codecommit:GetCommentsForComparedCommit",
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommit",
        "codecommit:GetCommitHistory",
        "codecommit:GetCommitsFromMergeBase",
        "codecommit:GetDifferences",
        "codecommit:GetFile",
        "codecommit:GetFolder",
        "codecommit:GetMergeCommit",
        "codecommit:GetMergeConflicts",
        "codecommit:GetMergeOptions",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetPullRequest",
        "codecommit:GetPullRequestApprovalStates",
        "codecommit:GetPullRequestOverrideState",
        "codecommit:GetReferences",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:GetTree",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:ListAssociatedApprovalRuleTemplatesForRepository",
        "codecommit:ListBranches",
        "codecommit:ListFileCommitHistory",
        "codecommit:ListPullRequests",
        "codecommit:ListTagsForResource",
```

```
        "codecommit:MergeBranchesByFastForward",
        "codecommit:MergeBranchesBySquash",
        "codecommit:MergeBranchesByThreeWay",
        "codecommit:MergePullRequestByFastForward",
        "codecommit:MergePullRequestBySquash",
        "codecommit:MergePullRequestByThreeWay",
        "codecommit:UpdateComment",
        "codecommit:UpdateDefaultBranch",
        "codecommit:UpdatePullRequestApprovalRuleContent",
        "codecommit:UpdatePullRequestApprovalState",
        "codecommit:UpdatePullRequestDescription",
        "codecommit:UpdatePullRequestStatus",
        "codecommit:UpdatePullRequestTitle",
        "codecommit:UpdateRepositoryDescription",
        "codecommit:PostCommentForComparedCommit",
        "codecommit:PostCommentForPullRequest",
        "codecommit:PostCommentReply",
        "codecommit:PutCommentReaction",
        "codecommit:PutFile"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CodeCommitKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:codecommit:id" : "false"
        },
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "codecommit.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CodeWhisperer",
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGlueCreateEni",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "true"
        },
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueENIonSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueENIonSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueNetwork",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws-glue-service-resource" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueEniOnInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDescribeGlueEni",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueKernelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "glue:ListSessions",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueCreateAndTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateDataQualityRuleset",
        "glue:CreateWorkflow",
        "glue:TagResource"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*",
        "arn:aws:glue:*:*:blueprint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:dataQualityRuleset/*",
        "arn:aws:glue:*:*:workflow/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "ProjectUserTag*"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true",
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
```

```
      }
    },
    {
      "Sid" : "GlueTagSessionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*",
        "arn:aws:glue:*:*:blueprint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:dataQualityRuleset/*",
        "arn:aws:glue:*:*:workflow/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*"
          ]
        },
        "ForAllValues:StringNotLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:*Session*",
        "glue:*Statement*",
        "glue:GetDashboardUrl",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
```

```
        "glue:PutWorkflowRunProperties",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:ResumeWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:StartJobRun",
        "glue:*DataQuality*",
        "glue:GetJobRun",
        "glue:GetJobRuns",
        "glue:BatchGetJobs",
        "glue:GetJob"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*",
        "arn:aws:glue:*:*:blueprint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:dataQualityRuleset/*",
        "arn:aws:glue:*:*:workflow/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GlueDQ",
      "Effect" : "Allow",
      "Action" : "glue:ListDataQuality*",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "GlueDQVetl",
      "Effect" : "Allow",
      "Action" : [
        "glue:*DataQuality*"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:dataQualityRuleset/dq_etl_ruleset_${aws:PrincipalTag/
AmazonDataZoneProject}_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "GlueListJobs",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListJobs"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueVisualETL",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetGeneratedCode"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueCompletions",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
```

```
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*",
        "arn:aws:glue:*:*:job/*"
      ]
    },
    {
      "Sid" : "GlueJobRunnerSessionLog",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws-glue/*"
    },
    {
      "Sid" : "EC2TagsForGlue",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "aws-glue-*"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueKmsPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/${aws:PrincipalTag/DefaultGlueCatalogKmsKeyId}",
        "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}"
      ],
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:glue_catalog_id" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "glue.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EMRS",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:AccessInteractiveEndpoints",
        "emr-serverless:AccessLivyEndpoints",
        "emr-serverless:GetApplication",
        "emr-serverless:StartApplication",
        "emr-serverless:StopApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:*Session*",
        "emr-serverless:GetResourceDashboard",
        "emr-serverless:TagResource",
        "emr-serverless:StartJobRun"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
```

```
    },
    {
      "Sid" : "AirflowActionsForTaggedEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "airflow:GetEnvironment",
        "airflow:UpdateEnvironment"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AirflowListEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "airflow:ListEnvironments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowUiApiAccess",
      "Effect" : "Allow",
      "Action" : [
        "airflow:CreateWebLoginToken",
        "airflow:InvokeRestApi"
      ],
      "Resource" : [
        "arn:aws:airflow:*:*:role/DataZoneMWAAEnv-${aws:PrincipalTag/
AmazonDataZoneDomain}-${aws:PrincipalTag/AmazonDataZoneProject}-${aws:PrincipalTag/
AmazonDataZoneScopeName}/User"
      ]
    },
    {
      "Sid" : "AirflowCloudwatchLogsActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogStreams",
```

```
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:airflow-DataZoneMWAAEnv-${aws:PrincipalTag/
AmazonDataZoneDomain}-${aws:PrincipalTag/AmazonDataZoneProject}-${aws:PrincipalTag/
AmazonDataZoneScopeName}-*"
      ]
    },
    {
      "Sid" : "AirflowCloudwatchActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : "AmazonMWAA"
        }
      }
    },
    {
      "Sid" : "GlueJobCWPutMetricActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : [
            "Glue",
            "AWS/Glue",
            "Glue Data Quality"
          ]
        }
      }
    },
    {
      "Sid" : "AirflowS3GetAccountPublicAccessBlock",
```

```
      "Effect" : "Allow",
      "Action" : "s3:GetAccountPublicAccessBlock",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowSqsActions",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:airflow-celery-*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketPublicAccessBlock"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "DataLakeS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataLakeCrossAccountS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:ListMultipartUploadParts",
        "s3:ListBucket"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataLakeCrossAccountKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:GetPublicKey",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "XAcctKmsDecrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:s3:arn"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "s3:prefix" : [
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}",
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
          ]
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/DomainBucketName" : ""
```

```
        }
      }
    },
    {
      "Sid" : "AirflowListDomainS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : ""
        }
      }
    },
    {
      "Sid" : "ListDomainBucketFromAthenaCatalog",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}"
      ],
      "Condition" : {
        "ArnEquals" : {
          "lambda:SourceFunctionArn" :
"arn:aws:lambda:*:*:function:athenafederatedcatalog_*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject",
```

```
        "s3:PutObjectRetention",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/DomainBucketName" : ""
        }
      }
    },
    {
      "Sid" : "S3BucketAcl",
      "Effect" : "Allow",
      "Action" : "s3:GetBucketAcl",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BREvalS3Tag",
      "Effect" : "Allow",
      "Action" : "s3:PutObjectTagging",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
genAI/assets/evaluations/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "s3:RequestObjectTagKeys" : [
            "BasicValidationStatus",
            "ContainsReferenceResponseForAllPrompts"
```

```
          ]
        },
        "StringEquals" : {
          "s3:RequestObjectTag/BasicValidationStatus" : [
            "valid",
            "invalid"
          ],
          "s3:RequestObjectTag/ContainsReferenceResponseForAllPrompts" : [
            "true",
            "false"
          ]
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/DomainBucketName" : ""
        }
      }
    },
    {
      "Sid" : "DomainS3BucketKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DZDomainKMSKeyXAcctPerm",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
```

```
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/DomainKmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:aws:datazone:domainId" : "${aws:PrincipalTag/
AmazonDataZoneDomain}"
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListLogGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueJobLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:PutLogEvents",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}/*"
      ]
    },
    {
      "Sid" : "ProjectLogGroup",
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}",
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}:log-stream:*"
      ]
    },
    {
      "Sid" : "CloudWatchStopQuery",
      "Effect" : "Allow",
      "Action" : [
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataLakeAthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:TerminateSession",
        "athena:CreatePreparedStatement",
        "athena:StopCalculationExecution",
        "athena:StartQueryExecution",
        "athena:UpdatePreparedStatement",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:UpdateNotebook",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:UpdateNotebookMetadata",
        "athena:DeleteNamedQuery",
        "athena:GetCalculationExecution",
        "athena:GetCalculationExecutionCode",
        "athena:GetCalculationExecutionStatus",
        "athena:GetNamedQuery",
```

```
        "athena:GetNotebookMetadata",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetSession",
        "athena:GetSessionStatus",
        "athena:GetWorkGroup",
        "athena:UpdateNamedQuery",
        "athena:CreateNamedQuery",
        "athena:ExportNotebook",
        "athena:StopQueryExecution",
        "athena:StartCalculationExecution",
        "athena:StartSession",
        "athena:CreatePresignedNotebookUrl",
        "athena:CreateNotebook",
        "athena:ImportNotebook",
        "athena:ListQueryExecutions",
        "athena:ListTagsForResource",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AthenaDataCatalogPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListTableMetadata"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:datacatalog/AwsDataCatalog",
        "arn:aws:athena:*:*:datacatalog/awsdatacatalog"
```

```
      ]
    },
    {
      "Sid" : "AthenaListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListWorkGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneUserPermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:CreateConnection",
        "datazone:DeleteConnection",
        "datazone:GetConnection",
        "datazone:GetDomain",
        "datazone:GetDomainExecutionRoleCredentials",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetProject",
        "datazone:GetUserProfile",
        "datazone:ListConnections",
        "datazone:ListEnvironments",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListProjects",
        "datazone:UpdateConnection",
        "datazone:PostLineageEvent",
        "datazone:*Compute*"
      ],
      "Resource" : "arn:aws:datazone:*:*:domain/${aws:PrincipalTag/
AmazonDataZoneDomain}"
    },
    {
      "Sid" : "CodeConnectionsUser",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection",
        "codeconnections:UseConnection",
        "codestar-connections:GetConnection",
        "codestar-connections:UseConnection"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "GlueGetDefaultDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default"
      ]
    },
    {
      "Sid" : "AllowGlueGetDatabasesExceptDefault",
      "Effect" : "Allow",
      "Action" : "glue:GetDatabases",
      "NotResource" : "arn:aws:glue:*:*:database/default",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GlueListDatabasesOnNoDatabases",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases"
      ],
      "Resource" : "arn:aws:glue:*:*:catalog"
    },
    {
      "Sid" : "GlueFileUploadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetClassifier",
        "glue:GetClassifiers",
```

```
        "glue:UseGlueStudio"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueProjectConnectionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:PassConnection",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:RefreshOAuth2Tokens"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GlueGetConnectionOnlyOnCatalog",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:RefreshOAuth2Tokens"
      ],
      "Resource" : "arn:aws:glue:*:*:catalog"
    },
    {
      "Sid" : "GlueDatalakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
```

```
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:GetCatalogImportStatus",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetDatabase",
        "glue:DeleteDatabase",
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:ListTableOptimizerRuns",
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:GetCatalogs",
        "glue:GetCatalog"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "S3TCatalogPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:*ColumnStatistics*",
        "glue:*Database*",
```

```
        "glue:*Partition*",
        "glue:*Table*",
        "glue:GetCatalog*",
        "glue:GetUserDefinedFunction*"
      ],
      "Resource" : "arn:*:glue:*:*:catalog/s3tablescatalog"
    },
    {
      "Sid" : "GlueCrawler",
      "Effect" : "Allow",
      "Action" : "glue:ListCrawls",
      "Resource" : "arn:aws:glue:*:*:crawler/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueGlobalTempDb",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/global_temp",
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "GlueDefaultCatalogs",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:UpdateCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
```

```
        }
      }
    },
    {
      "Sid" : "GlueNonDefaultCatalogs",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:UpdateCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GlueCatalogDb",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "LFforDL",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess",
        "lakeformation:GetResourceLFTags"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "IAMListRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "SetSourceIdentityForAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
```

```
    {
      "Sid" : "TagSessionForAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : "sts:TagSession",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneProject",
            "AmazonDataZoneDomain"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "${aws:PrincipalTag/
AmazonDataZoneDomain}",
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SetContextForTIP",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : [
        "arn:aws:sts::*:self"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "sqlworkbench.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "StsContext",
      "Effect" : "Allow",
      "Action" : "sts:SetContext",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:ArnEquals" : {
```

```
          "sts:RequestContextProviders" : [
            "arn:aws:iam::aws:contextProvider/IdentityCenter"
          ]
        },
        "Null" : {
          "sts:RequestContextProviders" : "false"
        }
      }
    },
    {
      "Sid" : "GlueConnectionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "UnrestrictedAccessGlueEntities",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListConnectionTypes",
        "glue:DescribeConnectionType"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueEntities",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListEntities",
        "glue:DescribeEntity",
        "glue:GetEntityRecords"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowPassRoleOnProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/${aws:PrincipalTag/RoleName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "airflow-serverless.amazonaws.com",
            "sagemaker.amazonaws.com",
            "glue.amazonaws.com",
            "airflow.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "elasticmapreduce.amazonaws.com",
            "scheduler.amazonaws.com",
            "access-grants.s3.amazonaws.com",
            "pods.eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SQLWorkBench",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:PutTab",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:ListTabs",
        "sqlworkbench:GetAutocompletion*",
        "sqlworkbench:PassAccountSettings",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:CreateConnection",
        "sqlworkbench:*QCustomContext",
        "sqlworkbench:GetQSql*",
        "sqlworkbench:GetSchemaInference"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "SQLWorkBenchActions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:AssociateNotebookWithTab",
      "Resource" : "arn:*:sqlworkbench:*:*:notebook/*"
    },
    {
      "Sid" : "SQLWorkBenchNotebookActions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateNotebook*",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook*",
        "sqlworkbench:DeleteNotebook*",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RSDataIAMSession",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
```

```
      "Sid" : "RedshiftDataActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ExistingRedshiftCompute",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetCredentials",
        "redshift:DescribeTags",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "true"
        },
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "RedshiftWithoutResourceType",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RSWgTagged",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift:DescribeTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "RSExistCatalog",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "arn:aws:redshift:*:*:dbname:*/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowListSecrets",
      "Effect" : "Allow",
```

```
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*"
    },
    {
      "Sid" : "ComputeCredentials",
      "Effect" : "Allow",
      "Action" : [
        "emr-containers:*ManagedEndpoint*",
        "emr-containers:TagResource",
        "emr-containers:DescribeSecurityConfiguration",
        "emr-containers:DescribeVirtualCluster",
        "redshift-serverless:GetCredentials",
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "RSDataMWg",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:GetStagingBucketLocation",
        "redshift-serverless:GetManagedWorkgroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "redshift-data:glue-catalog-arn" : "arn:aws:glue:*:*:catalog/*"
        }
      }
    },
    {
      "Sid" : "RssCreds",
      "Effect" : "Allow",
```

```
      "Action" : [
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "arn:aws:redshift-serverless:*:*:workgroup/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "redshift-data.amazonaws.com",
            "sqlworkbench.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowTagGetResources",
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowGetSecretForRedShift",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
```

```
      "Sid" : "CloudWatchMetricsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonQChatPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EMRClusterWithDataZoneTags",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetOnClusterAppUIPresignedURL",
        "elasticmapreduce:*Session*",
        "elasticmapreduce:AddTags"
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EMRClusterInfoPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "elasticmapreduce:ListReleaseLabels",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:CreatePersistentAppUI",
        "elasticmapreduce:DescribePersistentAppUI",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EMRGetClusterSessionCreds",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:GetClusterSessionCredentials"
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "elasticmapreduce:ExecutionRoleArn" : "arn:aws:iam::*:role/
${aws:PrincipalTag/RoleName}"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EmrContainersSSO",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "emr-containers.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "EMRPersistentAppUI",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:GetPersistentAppUIPresignedURL"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "elasticmapreduce:ExecutionRoleArn" : "arn:aws:iam::*:role/
${aws:PrincipalTag/RoleName}"
        }
      }
    },
    {
      "Sid" : "KmsWithEncrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "datazone.*.amazonaws.com",
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "bedrock.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "scheduler.*.amazonaws.com",
            "glue.*.amazonaws.com",
```

```
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EBDecrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "emr-serverless.*.amazonaws.com",
            "redshift.*.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "KmsManagement",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:RevokeGrant",
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "emr-serverless.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "codecommit.*.amazonaws.com",
            "scheduler.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AwsOwnedKmsKeyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
```

```
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AwsOwnedKmsManagement",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "EC2PermissionsForNotebookExecution",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "InvokeBRModel",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeModelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
```

```
        "ArnLike" : {
          "bedrock:InferenceProfileArn" : "arn:aws:bedrock:*:*:application-inference-
profile/*"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "InvokeBedrockModel",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BRInvokeAppProfile",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
```

```
      "Sid" : "AccessBedrockResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeAgent",
        "bedrock:Retrieve",
        "bedrock:ListIngestionJobs",
        "bedrock:StartIngestionJob",
        "bedrock:GetIngestionJob",
        "bedrock:ApplyGuardrail",
        "bedrock:ListPrompts",
        "bedrock:GetPrompt",
        "bedrock:CreatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:InvokeFlow",
        "bedrock:GetEvaluationJob",
        "bedrock:CreateEvaluationJob",
        "bedrock:StopEvaluationJob",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:ListTagsForResource",
        "bedrock:CreateAgentAlias",
        "bedrock:ListAgentAliases",
        "bedrock:GetAgentVersion",
        "bedrock:ListAgentVersions",
        "bedrock:DeleteAgentVersion",
        "bedrock:DeleteAgentAlias",
        "bedrock:GetAgentAlias",
        "bedrock:UpdateAgentAlias"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockResourceAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ApplyGuardrail",
        "bedrock:BatchDeleteEvaluationJob",
```

```
        "bedrock:CreateAgentAlias",
        "bedrock:CreateBlueprint",
        "bedrock:CreateBlueprintVersion",
        "bedrock:CreateDataAutomationProject",
        "bedrock:CreateEvaluationJob",
        "bedrock:CreatePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:DeleteAgentAlias",
        "bedrock:DeleteAgentVersion",
        "bedrock:DeleteBlueprint",
        "bedrock:DeleteDataAutomationProject",
        "bedrock:DeletePrompt",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentVersion",
        "bedrock:GetBlueprint",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataAutomationStatus",
        "bedrock:GetEvaluationJob",
        "bedrock:GetIngestionJob",
        "bedrock:GetPrompt",
        "bedrock:InvokeAgent",
        "bedrock:InvokeDataAutomationAsync",
        "bedrock:InvokeFlow",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentVersions",
        "bedrock:ListIngestionJobs",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "bedrock:Retrieve",
        "bedrock:StartIngestionJob",
        "bedrock:StopEvaluationJob",
        "bedrock:UpdateAgentAlias",
        "bedrock:UpdateBlueprint",
        "bedrock:UpdateDataAutomationProject",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentKnowledgeBases"
      ],
      "Resource" : "arn:aws:bedrock:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
```

```
      }
    },
    {
      "Sid" : "BREvalFM",
      "Effect" : "Allow",
      "Action" : "bedrock:CreateEvaluationJob",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*"
      ]
    },
    {
      "Sid" : "BRCreateEval",
      "Effect" : "Allow",
      "Action" : "bedrock:CreateEvaluationJob",
      "Resource" : [
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*::foundation-model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "InvokeDataAutomationAsyncPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeDataAutomationAsync"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:data-automation-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "InvokeBedrockInlineAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeInlineAgent",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "bedrock:InlineAgentName" : "${datazone:userId}"
        },
        "StringNotEquals" : {
          "bedrock:InlineAgentName" : ""
        }
      }
    },
    {
      "Sid" : "BedrockInvokeInlineAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeInlineAgent",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "bedrock:InlineAgentName" : "${datazone:userId}"
        },
        "StringNotEquals" : {
          "bedrock:InlineAgentName" : ""
        }
      }
    },
    {
      "Sid" : "BRRAG",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "ListBedrockEvaluationJobPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ListEvaluationJobs",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "BedrockNoResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListEvaluationJobs",
        "bedrock:RetrieveAndGenerate",
        "bedrock:ListFoundationModels"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "PassRoleToBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrockEvaluationRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*",
        "arn:aws:iam::*:role/AmazonBedrockServiceRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "iam:PassedToService" : [
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamPassRoleToBedrock",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrockEvaluationRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*",
        "arn:aws:iam::*:role/AmazonBedrockServiceRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "iam:PassedToService" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "TagBedrockResourcePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged",
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockTagResourcePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : "arn:aws:bedrock:*:*:*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonBedrockManaged",
```

```
            "AmazonDataZone*",
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "StringEqualsIfExists" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:arn" : "false"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KmsViaBedrockPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
```

```
      "Condition" : {
        "ForAllValues:StringLike" : {
          "kms:EncryptionContextKeys" : [
            "aws:bedrock*:arn",
            "aws:bedrock:guardrail-id"
          ]
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecretPermissionsForBedrockIDE",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerPermissionsForBedrock",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SecretKmsPermissionsForBedrockIDE",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:SecretARN" :
 "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "BRKmsSM",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:SecretARN" :
 "arn:aws:secretsmanager:*:*:secret:amazon-bedrock*"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
```

```
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InvokeFunctionForAmazonBedrockIDE",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "bedrock.amazonaws.com",
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "LambdaInvokeFunctionViaBedrock",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "bedrock.amazonaws.com",
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "DZEnvCfn",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplate",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/DataZone-Env-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CFNGetDataZoneEnvironmentStack",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/DataZone-Env-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GetGlueUserDefinedFuncLF",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GlueGetUserDefinedFunc",
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:userDefinedFunction/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataConnectionAllProjectResources",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "glue:GetConnections"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "DataConnectionLambdaLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/athenafederatedcatalog*"
    },
    {
      "Sid" : "DataConnOpen",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables",
        "glue:ManagedConnector",
        "glue:TestConnection",
```

```
        "codeconnections:GetHost",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codestar-connections:GetHost",
        "codestar-connections:ListConnections",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataConnectionEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Vpc" : "${aws:PrincipalTag/vpcArn}"
        }
      }
    },
    {
      "Sid" : "DataConnectionDeleteENI",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:*/*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ec2:Vpc" : "${aws:PrincipalTag/vpcArn}"
        }
      }
    },
    {
      "Sid" : "DataConnectionDescribeENI",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "PrivateECRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:CompleteLayerUpload",
        "ecr:DeleteRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:BatchDeleteImage",
        "ecr:ListTagsForResource",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:UploadLayerPart"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CreateECRRepositoryPermission",
      "Effect" : "Allow",
      "Action" : "ecr:CreateRepository",
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ECRTagResourcePermission",
      "Effect" : "Allow",
      "Action" : "ecr:TagResource",
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZoneProject",
            "ProjectUserTag*"
```

```
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "StringEqualsIfExists" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ECRUntagResourcePermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:UntagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "LFResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:ListPermissions",
        "lakeformation:DescribeResource",
        "ram:GetResourceShareInvitations",
        "lakeformation:CreateDataCellsFilter",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:DeleteDataCellsFilter",
        "lakeformation:GetDataCellsFilter",
```

```
        "lakeformation:UpdateDataCellsFilter",
        "ram:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "XAcctLFCreate",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        },
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        }
      }
    },
    {
      "Sid" : "XAcctRAMGlue",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteResourcePolicy",
        "glue:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "XAcctRAMLF",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:DeleteResourceShare",
        "ram:ListResourceSharePermissions",
        "ram:UpdateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        },
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        }
      }
    },
    {
      "Sid" : "RAMGetResourceSharesViaLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "XAcctRAMInvite",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share-invitation/*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*",
            "DataZoneS3AG*"
          ]
        }
      }
    },
    {
      "Sid" : "XAcctRAMLFHybrid",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ram:PermissionArn" : "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EventBridgeScheduleActions",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:CreateSchedule",
        "scheduler:GetSchedule",
        "scheduler:UpdateSchedule",
        "scheduler:DeleteSchedule"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EventBridgeScheduleGroupActions",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:GetScheduleGroup"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "QSFolderDS",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSource",
        "quicksight:DescribeFolder",
        "quicksight:DescribeFolderPermissions",
        "quicksight:ListFolderMembers"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:folder/*",
        "arn:aws:quicksight:*:*:datasource/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ManageQuickSightOtherResources",
```

```
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSet",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeUser",
        "quicksight:DescribeGroup"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:*"
      ]
    },
    {
      "Sid" : "ManagePassDataSourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:PassDataSource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:datasource/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ManageCreateDataSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSet",
        "quicksight:TagResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "StringEqualsIfExists" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CreateFolderMembership",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateFolderMembership"
      ],
      "Resource" : "arn:aws:quicksight:*:*:folder/sagemaker-*-assets",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneAssetsFolder" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioQueryExecutionRolePolicy

Deskripsi: Amazon SageMaker Studio menggunakan kebijakan ini saat menjalankan eksekusi kueri pada koneksi federasi.

`SageMakerStudioQueryExecutionRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioQueryExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 31 Januari 2025, 19:52 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioQueryExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueGetConnectionOnCatalog",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "GlueGetConnectionsForProject",
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetTags"
      ],
      "Resource" : "arn:aws:glue:*:*:connection/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "S3GetObjectForAthenaSpillBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/dzd*/*/dev/sys/athena/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true"
        }
      }
    },
    {
      "Sid" : "S3ListBucketOwnershipCheckForAthenaSpillBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true"
        }
      }
    },
    {
      "Sid" : "InvokeFunctionPermissionsForAthenaCatalogLambda",
      "Effect" : "Allow",
```

```
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceTag/federated_athena_datacatalog" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioUserIAMConsolePolicy

Deskripsi: Menyediakan hak istimewa penyiapan individual untuk Amazon SageMaker Unified Studio melalui Konsol Manajemen AWS dan SDK. Memungkinkan peluncuran SageMaker Unified Studio Portal.

`SageMakerStudioUserIAMConsolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioUserIAMConsolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Agustus 2025, 22:49 UTC
- Waktu teredit: 31 Maret 2026, 21:12 UTC

- ARN: `arn:aws:iam::aws:policy/SageMakerStudioUserIAMConsolePolicy`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:ListDomains",
        "datazone:GetDomain",
        "datazone:GetUserProfile",
        "datazone:ListProjects",
        "datazone:ListProjectProfiles",
        "datazone:CreateProject",
        "datazone:GetProject",
        "datazone:DeleteProject",
        "datazone:GetIamPortalLoginUrl",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironments",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetGroupProfile",
        "datazone:SearchGroupProfiles",
        "datazone:SearchUserProfiles",
        "datazone:ListProjectMemberships",
        "datazone:GetConnection",
        "datazone:ListConnections"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole",
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DataZoneKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioUserIAMDefaultExecutionPolicy

Deskripsi: Kebijakan eksekusi untuk menggunakan peran IAM dengan SageMaker Unified Studio. Memungkinkan pengguna mengakses sumber daya di akun lokal (tidak termasuk akses ke sumber daya data) untuk IAM-based penggunaan SageMaker Unified Studio.

`SageMakerStudioUserIAMDefaultExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioUserIAMDefaultExecutionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Agustus 2025, 17:19 UTC
- Waktu teredit: 13 Agustus 2026, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioUserIAMDefaultExecutionPolicy`

Versi kebijakan

Versi kebijakan: v29 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataZone",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:BatchUpdateNotifications",
```

```
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset*",
        "datazone:CreateConnection",
        "datazone:CreateEnvironment",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset*",
        "datazone:DeleteConnection",
        "datazone:DeleteEnvironment",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:Get*",
        "datazone:List*",
        "datazone:PostLineageEvent",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateConnection",
        "datazone:UpdateEnvironment",
        "datazone:UpdateProject",
        "datazone:UpdateSubscriptionRequest",
        "datazone:*Notebook*",
        "datazone:CreateCell",
        "datazone:UpdateCell",
        "datazone:DeleteCell",
        "datazone:BatchGetCell",
        "datazone:CreateCellRun",
        "datazone:UpdateCellRun",
        "datazone:DeleteCellRun",
        "datazone:BatchGetCellRun",
        "datazone:PutCellRunResult",
```

```
        "datazone:StartConversation",
        "datazone:GenerateCode",
        "datazone:SendMessage",
        "datazone:CancelMessage",
        "datazone:QueryGraph",
        "datazone:StartCompute",
        "datazone:StopCompute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "sts:AssumeRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
```

```
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless"
      ]
    },
    {
      "Sid" : "TagSession",
      "Effect" : "Allow",
      "Action" : "sts:TagSession",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "SourceIdentity",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "Q",
```

```
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "q:Get*",
        "q:List*",
        "q:PassRequest",
        "q:SendMessage",
        "q:StartConversation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter*"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
    },
    {
      "Sid" : "SageMakerUserTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteUserProfile",
        "sagemaker:UpdateUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SageMakerPrivateSpace",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
```

```
        "sagemaker:CreateSpace",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteSpace",
        "sagemaker:UpdateSpace"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:app/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "CanvasUserProfileApp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp",
        "sagemaker:CreateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/Canvas/*",
        "arn:aws:sagemaker:*:*:space/*/CanvasManagedSpace*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "AllowStartSessionForSpaceRemoteConnection",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:StartSession"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:Batch*",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sagemaker:Search",
        "sagemaker:*Endpoint*",
        "sagemaker:*Model*",
        "sagemaker:*Context*",
        "sagemaker:*Artifact*",
        "sagemaker:*Action*",
        "sagemaker:*Association*",
        "sagemaker:QueryLineage",
        "sagemaker:*InferenceComponent*",
        "sagemaker:*Job*",
        "sagemaker:*MlflowApp*",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker-mlflow:*",
        "sagemaker:*Feature*",
        "sagemaker:*Record"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerTagPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*",
            "sagemaker*",
            "sm-jumpstart*",
            "endpoint-has-jumpstart-model",
            "aws-jumpstart*",
            "Source",
            "CanvasModelName",
            "Canvas",
            "SageMaker",
            "ProjectS3Path",
            "Owner"
          ]
        },
        "ForAllValues:StringNotLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "sagemaker:shared-with:*"
          ]
        }
      }
    },
    {
      "Sid" : "LogsAndMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "cloudwatch:GetMetricData",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:Describe*",
        "logs:Get*",
        "logs:PutLogEvents",
```

```
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Glue",
      "Effect" : "Allow",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:CreateCatalog",
        "glue:Describe*",
        "glue:Get*",
        "glue:List*",
        "glue:NotifyEvent",
        "glue:RunStatement",
        "glue:StartCompletion",
        "glue:StopSession",
        "glue:UseGlueStudio",
        "glue:*Resource",
        "glue:*Job*",
        "glue:TestConnection",
        "glue:*DataQuality*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyForeignSessionAccess",
      "Effect" : "Deny",
      "Action" : [
        "athena:GetResourceDashboard",
        "athena:GetSession",
        "athena:GetSessionEndpoint",
        "athena:GetSessionStatus",
        "athena:StartSession",
        "athena:TerminateSession",
        "emr-serverless:*Session*",
        "emr-serverless:*Dashboard*",
        "emr-containers:*ManagedEndpoint*",
        "elasticmapreduce:*Session*",
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
```

```
        "glue:GetDashboardUrl",
        "glue:GetSession",
        "glue:GetSessionEndpoint",
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource",
        "emr-serverless:*Resource",
        "emr-containers:*Resource",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:RemoveTags",
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
```

```
        }
      }
    },
    {
      "Sid" : "GlueDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "GlueLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GrantPermissions",
        "lakeformation:ListResources",
        "lakeformation:ListPermissions",
        "lakeformation:RevokePermissions"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "SQLWorkBench",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftData",
      "Effect" : "Allow",
      "Action" : "redshift-data:*",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RedShiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:Describe*",
        "redshift-data:ExecuteStatement",
        "redshift-data:List*",
        "redshift-serverless:GetManagedWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
        "redshift:Describe*",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Bedrock",
      "Effect" : "Allow",
      "Action" : "bedrock:*",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/${aws:PrincipalTag/
AmazonDataZonePassedRolePath}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "bedrock.amazonaws.com",
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "sagemaker.amazonaws.com",
            "scheduler.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "elasticmapreduce.amazonaws.com",
            "redshift.amazonaws.com",
            "airflow-serverless.amazonaws.com",
            "events.amazonaws.com",
            "pods.eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AirflowServerless",
      "Effect" : "Allow",
      "Action" : [
        "airflow-serverless:List*",
        "airflow-serverless:Get*",
        "airflow-serverless:CreateWorkflow",
        "airflow-serverless:UpdateWorkflow",
        "airflow-serverless:DeleteWorkflow",
        "airflow-serverless:StartWorkflowRun",
        "airflow-serverless:StopWorkflowRun",
        "airflow-serverless:TagResource",
        "airflow-serverless:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowMWAA",
```

```
      "Effect" : "Allow",
      "Action" : [
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:CreateWebLoginToken",
        "airflow:InvokeRestApi"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3List",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CrossAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Scheduler",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:CreateSchedule",
        "scheduler:DeleteSchedule",
        "scheduler:Get*",
        "scheduler:List*",
        "scheduler:UpdateSchedule"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Athena",
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGet*",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:Get*",
        "athena:ImportNotebook",
        "athena:List*",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TagResource",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateSecret",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${datazone:projectId}"
        }
      }
    },
    {
      "Sid" : "SharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "GenerateRecommendations",
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ecr",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnectionsUser",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection",
        "codeconnections:UseConnection",
        "codestar-connections:GetConnection",
        "codestar-connections:UseConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "CodeConnectionsUserList",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetHost",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codestar-connections:GetHost",
        "codestar-connections:ListConnections",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
```

```
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3Kms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "AccessProjectS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject*",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject*",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/AmazonDataZoneProjectBucket}/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProjectBucket" : ""
        }
      }
    },
    {
```

```
      "Sid" : "EMR",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:Get*",
        "emr-serverless:List*",
        "emr-serverless:Start*",
        "emr-serverless:Access*Endpoints",
        "emr-serverless:Terminate*",
        "emr-serverless:*Resource",
        "emr-containers:*ManagedEndpoint*",
        "emr-containers:*SecurityConfiguration*",
        "emr-containers:*VirtualCluster*",
        "emr-containers:*Resource",
        "elasticmapreduce:*PersistentAppUI*",
        "elasticmapreduce:Start*",
        "elasticmapreduce:Get*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elasticmapreduce:Terminate*",
        "elasticmapreduce:*Tag*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CanvasGeneralPermissions",
      "Effect" : "Allow",
      "Action" : [
        "comprehend:BatchDetect*",
        "comprehend:Detect*",
        "textract:Analyze*",
        "textract:Start*",
        "textract:Get*",
        "rekognition:Detect*",
        "sagemaker-data-science-assistant:*",
        "rds:DescribeDBInstances",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScalingActivities",
        "quicksight:ListNamespaces",
        "events:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CanvasRedshiftAccess",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "CanvasEventBridgePutOperation",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "CanvasEventBridgeOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "CanvasEventBridgeTagBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SageMakerStudioUserIAMPermissiveExecutionPolicy

Deskripsi: Kebijakan eksekusi untuk menggunakan peran IAM dengan SageMaker Unified Studio. Memungkinkan pengguna mengakses sumber daya di akun Anda (termasuk akses luas ke semua API di layanan data seperti S3, Glue, CloudWatch Log, dan lainnya) untuk IAM-based penggunaan SageMaker Unified Studio.

`SageMakerStudioUserIAMPermissiveExecutionPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SageMakerStudioUserIAMPermissiveExecutionPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Agustus 2025, 17:19 UTC
- Waktu teredit: 13 Agustus 2026, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioUserIAMPermissiveExecutionPolicy`

Versi kebijakan

Versi kebijakan: v24 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:*",
        "glue:*",
        "logs:*",
        "redshift-data:*",
        "redshift-serverless:*",
        "redshift:*",
        "s3:*",
        "s3tables:*",
        "comprehend:*",
        "textract:*",
        "rekognition:*",
        "sagemaker-data-science-assistant:*",
        "rds:*",
        "quicksight:*",
        "events:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ComputeAccess",
      "Effect" : "Allow",
      "Action" : [
        "athena:*",
        "bedrock:*",
        "codewhisperer:*",
        "sagemaker-unified-studio-mcp:*",
```

```
        "elasticmapreduce:*",
        "emr-containers:*",
        "q:*",
        "sagemaker:*",
        "sagemaker-mlflow:*",
        "scheduler:*",
        "sqlworkbench:*",
        "emr-serverless:*",
        "airflow-serverless:*",
        "airflow:*",
        "application-autoscaling:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyForeignSessionAccess",
      "Effect" : "Deny",
      "Action" : [
        "athena:GetResourceDashboard",
        "athena:GetSession",
        "athena:GetSessionEndpoint",
        "athena:GetSessionStatus",
        "athena:StartSession",
        "athena:TerminateSession",
        "emr-serverless:*Session*",
        "emr-serverless:*Dashboard*",
        "emr-containers:*ManagedEndpoint*",
        "elasticmapreduce:*Session*",
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:GetDashboardUrl",
        "glue:GetSession",
        "glue:GetSessionEndpoint",
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
        "arn:aws:glue:*:*:session/*"
```

```
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource",
        "emr-serverless:*Resource",
        "emr-containers:*Resource",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:RemoveTags",
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DataZone",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:BatchUpdateNotifications",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset*",
```

```
        "datazone:CreateConnection",
        "datazone:CreateEnvironment",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset*",
        "datazone:DeleteConnection",
        "datazone:DeleteEnvironment",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:Get*",
        "datazone:List*",
        "datazone:PostLineageEvent",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateConnection",
        "datazone:UpdateEnvironment",
        "datazone:UpdateProject",
        "datazone:UpdateSubscriptionRequest",
        "datazone:*Notebook*",
        "datazone:CreateCell",
        "datazone:UpdateCell",
        "datazone:DeleteCell",
        "datazone:BatchGetCell",
        "datazone:CreateCellRun",
        "datazone:UpdateCellRun",
        "datazone:DeleteCellRun",
        "datazone:BatchGetCellRun",
        "datazone:PutCellRunResult",
        "datazone:StartConversation",
        "datazone:GenerateCode",
        "datazone:SendMessage",
```

```
        "datazone:CancelMessage",
        "datazone:QueryGraph",
        "datazone:StartCompute",
        "datazone:StopCompute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "sts:AssumeRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
```

```
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless"
      ]
    },
    {
      "Sid" : "TagSession",
      "Effect" : "Allow",
      "Action" : "sts:TagSession",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "lakeformation.amazonaws.com",
            "glue.amazonaws.com",
            "bedrock.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "scheduler.amazonaws.com",
```

```
            "emr-serverless.amazonaws.com",
            "elasticmapreduce.amazonaws.com",
            "airflow-serverless.amazonaws.com",
            "pods.eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SourceIdentity",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter*"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GrantPermissions",
        "lakeformation:ListResources",
        "lakeformation:ListPermissions",
        "lakeformation:RevokePermissions"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets",
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${datazone:projectId}"
        }
      }
    },
    {
      "Sid" : "SharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret",
```

```
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnectionsUser",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection",
        "codeconnections:UseConnection",
        "codestar-connections:GetConnection",
        "codestar-connections:UseConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "CodeConnectionsUserList",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetHost",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
```

```
        "codestar-connections:GetHost",
        "codestar-connections:ListConnections",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3Kms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
```

```
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
```

```
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SecretsManagerReadWrite

Deskripsi: Menye read/write diakan akses ke Manajer AWS Rahasia melalui Konsol Manajemen AWS. Catatan: ini tidak termasuk tindakan IAM, jadi gabungkan dengan IAMFullAccess jika konfigurasi rotasi diperlukan.

`SecretsManagerReadWrite`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SecretsManagerReadWrite` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 April 2018, 18:05 UTC
- Waktu teredit: 25 Agustus 2026, 23:37 UTC
- ARN: `arn:aws:iam::aws:policy/SecretsManagerReadWrite`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:*",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResource",
```

```
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys",
        "lambda:ListFunctions",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:SecretsManager*"
    },
    {
      "Sid" : "SARPermissions",
      "Effect" : "Allow",
      "Action" : [
        "serverlessrepo:CreateCloudFormationChangeSet",
        "serverlessrepo:GetApplication"
      ],
      "Resource" : "arn:aws:serverlessrepo:*:*:applications/SecretsManager*"
    },
    {
      "Sid" : "S3Permissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::awsserverlessrepo-changesets*",
        "arn:aws:s3:::secrets-manager-rotation-apps-*/*"
      ]
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateChangeSet",
            "ExecuteChangeSet"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SecurityAgentWebAppAPIPolicy

Deskripsi: Memberikan izin bagi pengguna yang diautentikasi untuk mengakses Aplikasi Web Agen Keamanan untuk mengonfigurasi dan menjalankan pengujian penetrasi keamanan otomatis. Kebijakan ini memungkinkan pengguna mengelola pentest, melihat temuan, memantau eksekusi

pengujian, dan berinteraksi dengan AWS sumber daya yang diperlukan untuk operasi pengujian keamanan.

`SecurityAgentWebAppAPIPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SecurityAgentWebAppAPIPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 02 Desember 2025, 15:04 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SecurityAgentWebAppAPIPolicy`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:ListAgentInstances",
        "securityagent:ListControls"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "AgentInstanceAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:AddArtifact",
        "securityagent:BatchDeletePentests",
        "securityagent:BatchGetAgentInstances",
        "securityagent:BatchGetArtifactMetadata",
        "securityagent:BatchGetFindings",
        "securityagent:BatchGetPentestJobs",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetSecurityTestContentMetadata",
        "securityagent:BatchGetTasks",
        "securityagent:CreateDocumentReview",
        "securityagent:CreatePentest",
        "securityagent:DeleteArtifact",
        "securityagent:DeleteDocumentReview",
        "securityagent:GetArtifact",
        "securityagent:GetCodeReviewTask",
        "securityagent:GetDocReviewTask",
        "securityagent:GetDocumentReview",
        "securityagent:GetDocumentReviewArtifact",
        "securityagent:ListArtifacts",
        "securityagent:ListControls",
        "securityagent:ListDiscoveredEndpoints",
        "securityagent:ListDocumentReviewComments",
        "securityagent:ListDocumentReviews",
        "securityagent:ListFindings",
        "securityagent:ListIntegratedResources",
        "securityagent:ListPentestJobsForPentest",
        "securityagent:ListPentests",
        "securityagent:ListTasks",
        "securityagent:StartCodeRemediation",
        "securityagent:StartPentestExecution",
        "securityagent:StopPentestExecution",
        "securityagent:UpdateFinding",
        "securityagent:UpdatePentest"
      ],
      "Resource" : "arn:aws:securityagent:*:*:agent-instance*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SecurityAgentWebAppPolicy

Deskripsi: Memberikan izin bagi pengguna yang diautentikasi untuk mengakses Aplikasi Web Agen Keamanan untuk mengonfigurasi dan menjalankan pengujian penetrasi keamanan otomatis. Kebijakan ini memungkinkan pengguna mengelola pentest, melihat temuan, memantau eksekusi pengujian, dan berinteraksi dengan AWS sumber daya yang diperlukan untuk operasi pengujian keamanan.

`SecurityAgentWebAppPolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SecurityAgentWebAppPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Februari 2026, 20:19 UTC
- Waktu teredit: 12 Februari 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/SecurityAgentWebAppPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:ListAgentSpaces",
        "securityagent:ListSecurityRequirements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AgentSpaceAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:AddArtifact",
        "securityagent:BatchDeletePentests",
        "securityagent:BatchGetAgentSpaces",
        "securityagent:BatchGetArtifactMetadata",
        "securityagent:BatchGetFindings",
        "securityagent:BatchGetPentestJobs",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetPentestJobContentMetadata",
        "securityagent:BatchGetPentestJobTasks",
        "securityagent:CreateDesignReview",
        "securityagent:CreatePentest",
        "securityagent:DeleteArtifact",
```

```
        "securityagent:GetArtifact",
        "securityagent:DeleteDesignReview",
        "securityagent:GetDesignReview",
        "securityagent:GetDesignReviewArtifact",
        "securityagent:ListArtifacts",
        "securityagent:ListSecurityRequirements",
        "securityagent:ListDiscoveredEndpoints",
        "securityagent:ListDesignReviewComments",
        "securityagent:ListDesignReviews",
        "securityagent:ListFindings",
        "securityagent:ListIntegratedResources",
        "securityagent:ListPentestJobsForPentest",
        "securityagent:ListPentests",
        "securityagent:ListPentestJobTasks",
        "securityagent:StartCodeRemediation",
        "securityagent:StartPentestJob",
        "securityagent:StopPentestJob",
        "securityagent:UpdateFinding",
        "securityagent:UpdatePentest"
      ],
      "Resource" : "arn:aws:securityagent:*:*:agent-space*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SecurityAudit

Deskripsi: Templat audit keamanan memberikan akses untuk membaca metadata konfigurasi keamanan. Ini berguna untuk perangkat lunak yang mengaudit konfigurasi sebuah Akun AWS.

`SecurityAudit`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SecurityAudit` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 30 September 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/SecurityAudit`

Versi kebijakan

Versi kebijakan: v94 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BaseSecurityAuditStatement",
      "Effect" : "Allow",
      "Action" : [
        "a4b:ListSkills",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
```

```
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListTagsForResource",
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetPrimaryEmail",
        "account:GetRegionOptStatus",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetPolicy",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags",
        "acm:Describe*",
        "acm:List*",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "amplify:GetWebACLForResource",
        "amplify:ListDomainAssociations",
        "amplify:ListResourcesForWebACL",
        "apigateway:GetPortal",
        "apigateway:GetPortalProduct",
        "apigateway:GetPortalProductSharingPolicy",
        "apigateway:GetRoutingRule",
        "apigateway:ListPortalProducts",
        "apigateway:ListPortals",
        "apigateway:ListProductPages",
        "apigateway:ListProductRestEndpointPages",
        "apigateway:ListRoutingRules",
        "appconfig:GetAccountSettings",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExperimentDefinition",
        "appconfig:GetExtension",
        "appconfig:GetExtensionAssociation",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListDeployments",
        "appconfig:ListEnvironments",
```

```
        "appconfig:ListExperimentDefinitions",
        "appconfig:ListExperimentRuns",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListExtensions",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:Describe*",
        "appmesh:Describe*",
        "appmesh:List*",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeCustomDomains",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListOperations",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appsync:GetApi",
        "appsync:GetApiCache",
        "appsync:GetChannelNamespace",
        "appsync:GetGraphqlApi",
        "appsync:GetIntrospectionSchema",
        "appsync:GetResourcePolicy",
        "appsync:GetSourceApiAssociation",
        "appsync:List*",
        "athena:GetWorkGroup",
        "athena:List*",
        "auditmanager:GetAccountStatus",
        "auditmanager:ListAssessmentControlInsightsByControlDomain",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessmentFrameworkShareRequests",
        "auditmanager:ListAssessmentReports",
        "auditmanager:ListAssessments",
        "auditmanager:ListControlDomainInsights",
        "auditmanager:ListControlDomainInsightsByAssessment",
        "auditmanager:ListControlInsightsByControlDomain",
```

```
        "auditmanager:ListControls",
        "auditmanager:ListNotifications",
        "auditmanager:ListTagsForResource",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling:Describe*",
        "backup:DescribeBackupVault",
        "backup:DescribeGlobalSettings",
        "backup:DescribeRegionSettings",
        "backup:GetBackupPlan",
        "backup:GetBackupPlanFromJSON",
        "backup:GetBackupPlanFromTemplate",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListProtectedResources",
        "backup:ListTags",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobDefinitions",
        "bedrock:CheckIngestedDocumentAcl",
        "bedrock:GetAccountDataRetention",
        "bedrock:GetAdvancedPromptOptimizationJob",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:GetAsyncInvoke",
        "bedrock:GetAutomatedReasoningPolicy",
        "bedrock:GetAutomatedReasoningPolicyBuildWorkflow",
        "bedrock:GetAutomatedReasoningPolicyNextScenario",
        "bedrock:GetBlueprint",
        "bedrock:GetBlueprintOptimizationStatus",
        "bedrock:GetBlueprintRecommendation",
        "bedrock:GetCustomModel",
        "bedrock:GetCustomModelDeployment",
        "bedrock:GetDataAutomationLibrary",
        "bedrock:GetDataAutomationLibraryIngestionJob",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataAutomationStatus",
        "bedrock:GetDataSource",
```

```
        "bedrock:GetEvaluationJob",
        "bedrock:GetExecutionFlowSnapshot",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowExecution",
        "bedrock:GetFlowVersion",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetGuardrail",
        "bedrock:GetImportedModel",
        "bedrock:GetInferenceProfile",
        "bedrock:GetIngestedDocumentAcl",
        "bedrock:GetIngestionJob",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetKnowledgeBaseDocuments",
        "bedrock:GetMarketplaceModelEndpoint",
        "bedrock:GetModelCopyJob",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelImportJob",
        "bedrock:GetModelInvocationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetPromptRouter",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:GetResourcePolicy",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListAgentVersions",
        "bedrock:ListCustomModels",
        "bedrock:ListDataSources",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlows",
        "bedrock:ListFlowVersions",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListImportedModels",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListIngestionJobs",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListMarketplaceModelEndpoints",
        "bedrock:ListModelCopyJobs",
        "bedrock:ListModelCustomizationJobs",
```

```
        "bedrock:ListModelImportJobs",
        "bedrock:ListModelInvocationJobs",
        "bedrock:ListPromptRouters",
        "bedrock:ListPrompts",
        "bedrock:ListProvisionedModelThroughputs",
        "bedrock:ListTagsForResource",
        "bedrock-agentcore:GetABTest",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetApiKeyCredentialProvider",
        "bedrock-agentcore:GetBatchEvaluation",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetBrowserProfile",
        "bedrock-agentcore:GetCodeInterpreter",
        "bedrock-agentcore:GetConfigurationBundle",
        "bedrock-agentcore:GetConfigurationBundleVersion",
        "bedrock-agentcore:GetEvaluator",
        "bedrock-agentcore:GetGateway",
        "bedrock-agentcore:GetGatewayTarget",
        "bedrock-agentcore:GetHarness",
        "bedrock-agentcore:GetMemory",
        "bedrock-agentcore:GetOauth2CredentialProvider",
        "bedrock-agentcore:GetOnlineEvaluationConfig",
        "bedrock-agentcore:GetPaymentConnector",
        "bedrock-agentcore:GetPaymentCredentialProvider",
        "bedrock-agentcore:GetPaymentInstrument",
        "bedrock-agentcore:GetPaymentManager",
        "bedrock-agentcore:GetPaymentSession",
        "bedrock-agentcore:GetPolicy",
        "bedrock-agentcore:GetPolicyEngine",
        "bedrock-agentcore:GetPolicyGeneration",
        "bedrock-agentcore:GetRecommendation",
        "bedrock-agentcore:GetRegistry",
        "bedrock-agentcore:GetRegistryRecord",
        "bedrock-agentcore:GetResourcePolicy",
        "bedrock-agentcore:GetTokenVault",
        "bedrock-agentcore:ListABTests",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimeVersions",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListApiKeyCredentialProviders",
        "bedrock-agentcore:ListBatchEvaluations",
        "bedrock-agentcore:ListBrowserProfiles",
        "bedrock-agentcore:ListBrowsers",
```

```
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListConfigurationBundleVersions",
        "bedrock-agentcore:ListConfigurationBundles",
        "bedrock-agentcore:ListEvaluators",
        "bedrock-agentcore:ListGatewayTargets",
        "bedrock-agentcore:ListGateways",
        "bedrock-agentcore:ListHarnesses",
        "bedrock-agentcore:ListMemories",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "bedrock-agentcore:ListOnlineEvaluationConfigs",
        "bedrock-agentcore:ListPaymentConnectors",
        "bedrock-agentcore:ListPaymentCredentialProviders",
        "bedrock-agentcore:ListPaymentInstruments",
        "bedrock-agentcore:ListPaymentManagers",
        "bedrock-agentcore:ListPaymentSessions",
        "bedrock-agentcore:ListPolicies",
        "bedrock-agentcore:ListPolicyEngines",
        "bedrock-agentcore:ListPolicyGenerationAssets",
        "bedrock-agentcore:ListPolicyGenerations",
        "bedrock-agentcore:ListRecommendations",
        "bedrock-agentcore:ListRegistries",
        "bedrock-agentcore:ListRegistryRecords",
        "bedrock-agentcore:ListTagsForResource",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "chime:List*",
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaborationConfiguredAudienceModelAssociation",
        "cleanrooms:GetCollaborationIdNamespaceAssociation",
        "cleanrooms:GetCollaborationPrivacyBudgetTemplate",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetConfiguredTableAssociationAnalysisRule",
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
```

```
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborationIdNamespaceAssociations",
        "cleanrooms:ListCollaborationPrivacyBudgets",
        "cleanrooms:ListCollaborationPrivacyBudgetTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredAudienceModelAssociations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgets",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:PreviewPrivacyImpact",
        "cloud9:Describe*",
        "cloud9:ListEnvironments",
        "clouddirectory:ListDirectories",
        "cloudformation:DescribeStack*",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ListStackResources",
        "cloudformation:ListStack*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudsearch:DescribeDomainEndpointOptions",
        "cloudsearch:DescribeDomains",
        "cloudsearch:DescribeServiceAccessPolicies",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
```

```
        "cloudtrail:ListTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetrics",
        "cloudwatch:ListTagsForResource",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact:ListPackages",
        "codeartifact:ListRepositories",
        "codebuild:BatchGetProjects",
        "codebuild:GetResourcePolicy",
        "codebuild:ListProjects",
        "codebuild:ListSourceCredentials",
        "codecommit:BatchGetRepositories",
        "codecommit:GetBranch",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:List*",
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:GetJobDetails",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineExecution",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelines",
        "codestar:Describe*",
        "codestar:List*",
        "cognito-identity:Describe*",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentities",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:Describe*",
        "cognito-idp:ListDevices",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
```

```
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserImportJobs",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListUsersInGroup",
        "cognito-sync:Describe*",
        "cognito-sync:List*",
        "comprehend:Describe*",
        "comprehend:List*",
        "comprehendmedical:ListICD10CMInferenceJobs",
        "comprehendmedical:ListPHIDetectionJobs",
        "comprehendmedical:ListRxNormInferenceJobs",
        "comprehendmedical:ListSNOMEDCTInferenceJobs",
        "config:BatchGetAggregateResourceConfig",
        "config:BatchGetResourceConfig",
        "config:Deliver*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:SelectAggregateResourceConfig",
        "config:SelectResourceConfig",
        "connect:ListApprovedOrigins",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListLambdaFunctions",
        "connect:ListLexBots",
        "connect:ListSecurityKeys",
        "databrew:DescribeDataset",
        "databrew:DescribeProject",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "dataexchange:ListDataSets",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:EvaluateExpression",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "datapipeline:ValidatePipelineDefinition",
        "datasync:Describe*",
        "datasync:List*",
```

```
        "dax:Describe*",
        "dax:ListTags",
        "deepracer:ListModels",
        "detective:GetGraphIngestState",
        "detective:ListGraphs",
        "detective:ListMembers",
        "devicefarm:ListProjects",
        "directconnect:Describe*",
        "discovery:DescribeAgents",
        "discovery:DescribeConfigurations",
        "discovery:DescribeContinuousExports",
        "discovery:DescribeExportConfigurations",
        "discovery:DescribeExportTasks",
        "discovery:DescribeImportTasks",
        "dlm:GetLifecyclePolicies",
        "dlm:GetLifecyclePolicy",
        "dlm:ListTagsForResource",
        "dms:Describe*",
        "dms:ListTagsForResource",
        "docdb-elastic:ListClusters",
        "ds:DescribeDirectories",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeEndpoints",
        "dynamodb:DescribeExport",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeImport",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetAbacStatus",
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListBackups",
        "dynamodb:ListContributorInsights",
        "dynamodb:ListExports",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListImports",
```

```
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:GetActiveVpnTunnelStatus",
        "ec2:GetAllowedImagesSettings",
        "ec2:GetAssociatedEnclaveCertificateIamRoles",
        "ec2:GetAssociatedIpv6PoolCidrs",
        "ec2:GetCapacityManagerAttributes",
        "ec2:GetCapacityManagerMetricDimensions",
        "ec2:GetCapacityManagerMonitoredTagKeys",
        "ec2:GetCapacityReservationUsage",
        "ec2:GetCoipPoolUsage",
        "ec2:GetDeclarativePoliciesReportSummary",
        "ec2:GetDefaultCreditSpecification",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEnabledIpamPolicy",
        "ec2:GetFlowLogsIntegrationTemplate",
        "ec2:GetGroupsForCapacityReservation",
        "ec2:GetHostReservationPurchasePreview",
        "ec2:GetImageAncestry",
        "ec2:GetImageBlockPublicAccessState",
        "ec2:GetInstanceMetadataDefaults",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamAddressHistory",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "ec2:GetIpamDiscoveredRoutes",
        "ec2:GetIpamInternetRegistryAssociationAsns",
        "ec2:GetIpamInternetRegistryAssociationCidrs",
        "ec2:GetIpamPolicyAllocationRules",
        "ec2:GetIpamPolicyOrganizationTargets",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetIpamPrefixListResolverRules",
        "ec2:GetIpamPrefixListResolverVersions",
        "ec2:GetIpamResourceCidrs",
        "ec2:GetIpamRouteOriginAuthorizations",
        "ec2:GetIpamRouteProtectionFindings",
        "ec2:GetIpamRoutingPolicyRegistrations",
        "ec2:GetManagedPrefixListAssociations",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetManagedResourceVisibility",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
```

```
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetReservedInstancesExchangeQuote",
        "ec2:GetResourcePolicy",
        "ec2:GetRouteServerAssociations",
        "ec2:GetRouteServerPropagations",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:GetSerialConsoleAccessStatus",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetSpotPlacementScores",
        "ec2:GetSubnetCidrReservations",
        "ec2:GetTransitGatewayAttachmentPropagations",
        "ec2:GetTransitGatewayMeteringPolicyEntries",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayPolicyTableAssociations",
        "ec2:GetTransitGatewayPolicyTableEntries",
        "ec2:GetTransitGatewayPrefixListReferences",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessEndpointTargets",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:GetVpcResourcesBlockingEncryptionEnforcement",
        "ec2:GetVpnConnectionDeviceTypes",
        "ec2:GetVpnTunnelReplacementStatus",
        "ec2:ListImagesInRecycleBin",
        "ec2:ListSnapshotsInRecycleBin",
        "ec2:ListVolumesInRecycleBin",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:SearchTransitGatewayRoutes",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribeImages",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
```

```
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecs:Describe*",
        "ecs:List*",
        "eks:DescribeAccessEntry",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodeGroup",
        "eks:ListAccessEntries",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListNodeGroups",
        "eks:ListTagsForResource",
        "eks:ListUpdates",
        "elasticache:Describe*",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:ListTagsForResource",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
```

```
        "elastictranscoder:ListPipelines",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "entityresolution:GetIdNamespace",
        "es:Describe*",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListElasticsearchInstanceTypeDetails",
        "es:ListElasticsearchVersions",
        "es:ListTags",
        "events:Describe*",
        "events:List*",
        "events:TestEventPattern",
        "finspace:ListEnvironments",
        "finspace:ListKxEnvironments",
        "firehose:Describe*",
        "firehose:List*",
        "fms:ListComplianceStatus",
        "fms:ListPolicies",
        "forecast:ListDatasets",
        "frauddetector:GetDetectors",
        "fsx:Describe*",
        "fsx:List*",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "geo:ListMaps",
        "glacier:DescribeJob",
        "glacier:DescribeVault",
        "glacier:GetDataRetrievalPolicy",
        "glacier:GetVaultAccessPolicy",
        "glacier:GetVaultLock",
        "glacier:GetVaultNotifications",
        "glacier:ListJobs",
        "glacier:ListTagsForVault",
        "glacier:ListVaults",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:GetCrawlers",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDevEndpoints",
```

```
        "glue:GetJobBookmark",
        "glue:GetJobRuns",
        "glue:GetJobs",
        "glue:GetResourcePolicies",
        "glue:GetResourcePolicy",
        "glue:GetSchema",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:GetTags",
        "glue:ListJobs",
        "glue:ListSchemaVersions",
        "glue:ListSchemas",
        "glue:ListSessions",
        "grafana:ListWorkspaces",
        "greengrass:List*",
        "guardduty:DescribeMalwareScans",
        "guardduty:DescribeOrganizationConfiguration",
        "guardduty:DescribePublishingDestination",
        "guardduty:Get*",
        "guardduty:List*",
        "health:DescribeAffectedAccountsForOrganization",
        "health:DescribeAffectedEntities",
        "health:DescribeAffectedEntitiesForOrganization",
        "health:DescribeEntityAggregates",
        "health:DescribeEventAggregates",
        "health:DescribeEventDetails",
        "health:DescribeEventDetailsForOrganization",
        "health:DescribeEvents",
        "health:DescribeEventsForOrganization",
        "health:DescribeEventTypes",
        "health:DescribeHealthServiceStatusForOrganization",
        "healthlake:ListFHIRDatastores",
        "honeycode:ListTables",
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy",
        "identitystore:DescribeGroupMembership",
```

```
        "identitystore:GetGroupId",
        "identitystore:GetGroupMembershipId",
        "identitystore:GetUserId",
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "identitystore:ListUsers",
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "inspector2:BatchGetAccountStatus",
        "inspector2:BatchGetFreeTrialInfo",
        "inspector2:DescribeOrganizationConfiguration",
        "inspector2:GetConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:GetFindingsReportStatus",
        "inspector2:GetMember",
        "inspector2:ListAccountPermissions",
        "inspector2:ListCoverage",
        "inspector2:ListCoverageStatistics",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:ListFilters",
        "inspector2:ListFindingAggregations",
        "inspector2:ListFindings",
        "inspector2:ListTagsForResource",
        "inspector2:ListUsageTotals",
        "iot:Describe*",
        "iot:GetPolicy",
        "iot:GetPolicyVersion",
        "iot:List*",
        "iotanalytics:ListChannels",
        "iotevents:ListInputs",
        "iotfleetwise:ListModelManifests",
        "iotsitewise:DescribeGatewayCapabilityConfiguration",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListGateways",
        "iottwinmaker:ListWorkspaces",
        "kafka-cluster:Describe*",
        "kafka:Describe*",
        "kafka:GetBootstrapBrokers",
        "kafka:GetCompatibleKafkaVersions",
        "kafka:List*",
```

```
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kendra:DescribeIndex",
        "kendra:ListDataSources",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeLimits",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListShards",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeEdgeConfiguration",
        "kinesisvideo:DescribeMappedResourceConfiguration",
        "kinesisvideo:DescribeMediaStorageConfiguration",
        "kinesisvideo:DescribeNotificationConfiguration",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lambda:GetAccountSettings",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetResourcePolicy",
        "lambda:GetRuntimeManagementConfig",
        "lambda:List*",
        "lex:DescribeBot",
        "lex:DescribeResourcePolicy",
        "lex:ListBots",
```

```
        "license-manager:List*",
        "lightsail:GetBuckets",
        "lightsail:GetContainerServices",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetInstancePortStates",
        "lightsail:GetInstances",
        "lightsail:GetLoadBalancers",
        "lightsail:GetStaticIps",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "lookoutequipment:ListDatasets",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutvision:ListProjects",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:ListApplications",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "machinelearning:DescribeMLModels",
        "macie2:ListFindings",
        "managedblockchain:ListNetworks",
        "mechanicalturk:ListHITs",
        "mediaconnect:Describe*",
        "mediaconnect:List*",
        "medialive:ListChannels",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage:DescribeOriginEndpoint",
        "mediapackage:ListOriginEndpoints",
        "mediastore:DescribeContainer",
        "mediastore:GetContainerPolicy",
        "mediastore:GetCorsPolicy",
        "mediastore:GetLifecyclePolicy",
        "mediastore:ListContainers",
        "mediastore:ListTagsForResource",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeUsers",
        "mq:DescribeBroker",
        "mq:DescribeBrokerEngineTypes",
```

```
        "mq:DescribeBrokerInstanceOptions",
        "mq:DescribeConfiguration",
        "mq:DescribeConfigurationRevision",
        "mq:DescribeUser",
        "mq:ListBrokers",
        "mq:ListConfigurationRevisions",
        "mq:ListConfigurations",
        "mq:ListTags",
        "mq:ListUsers",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "networkmanager:DescribeGlobalNetworks",
        "nimble:ListStudios",
        "opsworks-cm:DescribeServers",
        "opsworks:DescribeStacks",
        "organizations:Describe*",
        "organizations:List*",
        "pcs:GetCluster",
        "pcs:GetComputeNodeGroup",
        "pcs:GetQueue",
        "pcs:ListClusters",
        "pcs:ListComputeNodeGroups",
        "pcs:ListQueues",
        "pcs:ListTagsForResource",
        "personalize:DescribeDatasetGroup",
        "personalize:ListDatasetGroups",
        "private-networks:ListNetworks",
        "profile:GetDomain",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "qapps:GetQApp",
        "qapps:ListQApps",
        "qapps:ListTagsForResource",
        "qbusiness:GetApplication",
        "qbusiness:GetDataSource",
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetPolicy",
```

```
        "qbusiness:GetRetriever",
        "qbusiness:GetWebExperience",
        "qbusiness:ListApplications",
        "qbusiness:ListDataSources",
        "qbusiness:ListDataSourceSyncJobs",
        "qbusiness:ListDocuments",
        "qbusiness:ListGroups",
        "qbusiness:ListIndices",
        "qbusiness:ListPlugins",
        "qbusiness:ListRetrievers",
        "qbusiness:ListSubscriptions",
        "qbusiness:ListTagsForResource",
        "qbusiness:ListWebExperiences",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:ListLedgers",
        "quicksight:Describe*",
        "quicksight:List*",
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares",
        "ram:List*",
        "rds:Describe*",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetResourcePolicy",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:Describe*",
        "rekognition:Describe*",
        "rekognition:List*",
        "resource-groups:ListGroupResources",
        "robomaker:Describe*",
        "robomaker:List*",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
```

```
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53:Get*",
        "route53:List*",
        "route53domains:GetDomainDetail",
        "route53domains:GetOperationDetail",
        "route53domains:ListDomains",
        "route53domains:ListOperations",
        "route53domains:ListTagsForDomain",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3-object-lambda:GetObjectAcl",
        "s3-object-lambda:GetObjectVersionAcl",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListOutpostsWithS3",
        "s3-outposts:ListSharedEndpoints",
        "s3:DescribeJob",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrantsInstanceResourcePolicy",
        "s3:GetAccessPoint",
        "s3:GetAccessPointConfigurationForObjectLambda",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucket*",
        "s3:GetEncryptionConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensGroup",
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsInstances",
```

```
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListCallerAccessGrants",
        "s3:ListJobs",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:ListAllMyDirectoryBuckets",
        "s3files:GetAccessPoint",
        "s3files:GetFileSystem",
        "s3files:GetFileSystemPolicy",
        "s3files:GetMountTarget",
        "s3files:GetSynchronizationConfiguration",
        "s3files:ListAccessPoints",
        "s3files:ListFileSystems",
        "s3files:ListMountTargets",
        "s3files:ListTagsForResource",
        "s3tables:GetNamespace",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableMaintenanceConfiguration",
        "s3tables:GetTablePolicy",
        "s3tables:ListNamespaces",
        "s3tables:ListTableBuckets",
        "s3tables:ListTables",
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:GetVectors",
        "s3vectors:ListIndexes",
        "s3vectors:ListVectorBuckets",
        "s3vectors:ListVectors",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
```

```
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:ListTagsForResource",
        "sdb:DomainMetadata",
        "sdb:ListDomains",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityhub:BatchGetAutomationRules",
        "securityhub:BatchGetConfigurationPolicyAssociations",
        "securityhub:BatchGetControlEvaluations",
        "securityhub:BatchGetEnabledRegionsV2",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:Describe*",
        "securityhub:Get*",
        "securityhub:List*",
        "security-ir:BatchGetMemberAccountDetails",
        "security-ir:GetCase",
        "security-ir:GetCaseAttachmentDownloadUrl",
        "security-ir:GetMembership",
        "security-ir:ListCaseEdits",
        "security-ir:ListCases",
        "security-ir:ListComments",
        "security-ir:ListInvestigations",
        "security-ir:ListMemberships",
        "security-ir:ListTagsForResource",
        "serverlessrepo:GetApplicationPolicy",
        "serverlessrepo:List*",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "servicequotas:ListTagsForResource",
        "ses:Describe*",
```

```
        "ses:GetAccount",
        "ses:GetAccountSendingEnabled",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetDedicatedIps",
        "ses:GetEmailIdentity",
        "ses:GetIdentityDkimAttributes",
        "ses:GetIdentityPolicies",
        "ses:GetIdentityVerificationAttributes",
        "ses:ListConfigurationSets",
        "ses:ListDedicatedIpPools",
        "ses:ListIdentities",
        "ses:ListIdentityPolicies",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListVerifiedEmailAddresses",
        "shield:Describe*",
        "shield:GetSubscriptionState",
        "shield:List*",
        "snowball:ListClusters",
        "snowball:ListJobs",
        "sns:GetDataProtectionPolicy",
        "sns:GetPlatformApplicationAttributes",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm:Describe*",
        "ssm:GetAutomationExecution",
        "ssm:GetServiceSetting",
        "ssm:ListAssociations",
        "ssm:ListAssociationVersions",
        "ssm:ListCommands",
        "ssm:ListComplianceItems",
        "ssm:ListComplianceSummaries",
        "ssm:ListDocumentMetadataHistory",
        "ssm:ListDocuments",
        "ssm:ListDocumentVersions",
```

```
        "ssm:ListInventoryEntries",
        "ssm:ListOpsMetadata",
        "ssm:ListResourceComplianceSummaries",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "sso:DescribeAccountAssignmentCreationStatus",
        "sso:DescribeAccountAssignmentDeletionStatus",
        "sso:DescribeApplication",
        "sso:DescribeApplicationAssignment",
        "sso:DescribeApplicationProvider",
        "sso:DescribeInstance",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:DescribePermissionSetProvisioningStatus",
        "sso:DescribeRegion",
        "sso:DescribeTrustedTokenIssuer",
        "sso:GetApplicationAccessScope",
        "sso:GetApplicationAssignmentConfiguration",
        "sso:GetApplicationAuthenticationMethod",
        "sso:GetApplicationGrant",
        "sso:GetApplicationSessionConfiguration",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetPermissionsBoundaryForPermissionSet",
        "sso:ListAccountAssignmentCreationStatus",
        "sso:ListAccountAssignmentDeletionStatus",
        "sso:ListAccountAssignments",
        "sso:ListAccountAssignmentsForPrincipal",
        "sso:ListAccountsForProvisionedPermissionSet",
        "sso:ListApplicationAccessScopes",
        "sso:ListApplicationAssignments",
        "sso:ListApplicationAssignmentsForPrincipal",
        "sso:ListApplicationAuthenticationMethods",
        "sso:ListApplicationGrants",
        "sso:ListApplicationInstanceCertificates",
        "sso:ListApplicationInstances",
        "sso:ListApplicationProviders",
        "sso:ListApplications",
        "sso:ListApplicationTemplates",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListDirectoryAssociations",
        "sso:ListInstances",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSetProvisioningStatus",
        "sso:ListPermissionSets",
```

```
        "sso:ListPermissionSetsProvisionedToAccount",
        "sso:ListProfileAssociations",
        "sso:ListProfiles",
        "sso:ListRegions",
        "sso:ListTagsForResource",
        "sso:ListTrustedTokenIssuers",
        "sso-directory:ListExternalIdPConfigurationsForDirectory",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "states:ListTagsForResource",
        "storagegateway:DescribeBandwidthRateLimit",
        "storagegateway:DescribeCache",
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:DescribeMaintenanceStartTime",
        "storagegateway:DescribeNFSFileShares",
        "storagegateway:DescribeSMBSettings",
        "storagegateway:DescribeSnapshotSchedule",
        "storagegateway:DescribeStorediSCSIVolumes",
        "storagegateway:DescribeTapeArchives",
        "storagegateway:DescribeTapeRecoveryPoints",
        "storagegateway:DescribeTapes",
        "storagegateway:DescribeUploadBuffer",
        "storagegateway:DescribeVTLDevices",
        "storagegateway:DescribeWorkingStorage",
        "storagegateway:List*",
        "sts:GetAccessKeyInfo",
        "support:DescribeTrustedAdvisorCheckRefreshStatuses",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeTrustedAdvisorChecks",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "tag:GetTagKeys",
        "tiros:GetQueryAnswer",
```

```
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts",
        "transcribe:GetCallAnalyticsCategory",
        "transcribe:GetMedicalVocabulary",
        "transcribe:GetVocabulary",
        "transcribe:GetVocabularyFilter",
        "transcribe:ListCallAnalyticsCategories",
        "transcribe:ListCallAnalyticsJobs",
        "transcribe:ListLanguageModels",
        "transcribe:ListMedicalTranscriptionJobs",
        "transcribe:ListMedicalVocabularies",
        "transcribe:ListTagsForResource",
        "transcribe:ListTranscriptionJobs",
        "transcribe:ListVocabularies",
        "transcribe:ListVocabularyFilters",
        "transfer:Describe*",
        "transfer:List*",
        "translate:List*",
        "trustedadvisor:Describe*",
        "voiceid:DescribeDomain",
        "waf-regional:GetWebACL",
        "waf-regional:ListResourcesForWebACL",
        "waf-regional:ListTagsForResource",
        "waf-regional:ListWebACLs",
        "waf:GetWebACL",
        "waf:ListTagsForResource",
        "waf:ListWebACLs",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:ListIPSets",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRegexPatternSets",
        "wafv2:ListResourcesForWebACL",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "wafv2:ListWebACLs",
        "wisdom:GetAssistant",
        "wisdom:ListAssistants",
        "workdocs:DescribeResourcePermissions",
        "workspaces:Describe*",
        "xray:GetEncryptionConfig",
        "xray:GetGroup",
```

```
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetTraceSummaries",
        "xray:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/cors",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/exports/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses/*",
```

```
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/tags/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SecurityLakeResourceManagementServiceRolePolicy

Deskripsi: Menyediakan akses untuk mengelola sumber daya yang dibuat oleh Security Lake.

`SecurityLakeResourceManagementServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 14 November 2024, 22:10 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeResourceManagementServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadEventBridgeRules",
      "Effect" : "Allow",
      "Action" : [
        "events:ListRules"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecurityLakeEventRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AmazonSecurityLake-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "ManageSecurityLakeLambdaConfigurations",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:PutFunctionConcurrency",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetFunctionConcurrency",
        "lambda:GetRuntimeManagementConfig",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:PublishVersion",
        "lambda:DeleteFunctionConcurrency",
        "lambda:DeleteEventSourceMapping",
        "lambda:GetAlias",
        "lambda:GetPolicy",
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DeletePartitionUpdaterLambda",
      "Effect" : "Allow",
      "Action" : "lambda:DeleteFunction",
      "Resource" :
 "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListLambdaEventSourceMappings",
      "Effect" : "Allow",
```

```
      "Action" : [
        "lambda:ListEventSourceMappings"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowUpdateLambdaEventSourceMapping",
      "Effect" : "Allow",
      "Action" : [
        "lambda:UpdateEventSourceMapping"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "lambda:FunctionArn" :
 "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*"
        }
      }
    },
    {
      "Sid" : "AllowUpdateLambdaConfigs",
      "Effect" : "Allow",
      "Action" : [
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-
*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecurityLakeGlueResources",
      "Effect" : "Allow",
```

```
      "Action" : [
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:GetTable",
        "glue:GetTables",
        "glue:UpdateTable",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDataLakeConfigurationManagement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObjectAttributes",
        "s3:GetBucketNotification",
        "s3:PutBucketNotification",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:GetEncryptionConfiguration",
        "s3:GetReplicationConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMetaDataCompactionAndManagement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.avro",
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.metadata.json"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReadSecurityLakeLambdaLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:GetQueryResults",
        "logs:GetLogRecord"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLakeMetastoreManager-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecurityLakeSQSQueue",
      "Effect" : "Allow",
      "Action" : [
        "sqs:StartMessageMoveTask",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ChangeMessageVisibility",
```

```
        "sqs:ListMessageMoveTasks",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:SecurityLake_*",
        "arn:aws:sqs:*:*:AmazonSecurityLakeManager-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDataLakeManagement",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SecurityLakeServiceLinkedRole

Deskripsi: Kebijakan ini memberikan izin untuk mengoperasikan layanan Amazon Security Lake atas nama Anda

`SecurityLakeServiceLinkedRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 29 November 2022, 14:03 UTC
- Waktu teredit: 15 Juli 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsPolicies",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeOrgAccounts",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/o-*/*"
      ]
    },
    {
      "Sid" : "AllowManagementOfServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel",
        "cloudtrail:GetServiceLinkedChannel",
        "cloudtrail:UpdateServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/security-lake/*"
    },
    {
      "Sid" : "AllowListServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListServiceLinkedChannels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrganizationTrailValidation",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetEventSelectors"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "DescribeAnyVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListDelegatedAdmins",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowWafLoggingConfiguration",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:ListLoggingConfigurations",
        "wafv2:DeleteLoggingConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "wafv2:LogScope" : "SecurityLake"
        }
      }
    },
    {
      "Sid" : "AllowPutLoggingConfiguration",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "ArnLike" : {
          "wafv2:LogDestinationResource" : "arn:aws:s3:::aws-waf-logs-security-lake-*"
        }
      }
    },
    {
      "Sid" : "ListWebACLs",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:ListWebACLs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LogDelivery",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ServerMigration_ServiceRole

Deskripsi: Izin untuk mengiz AWS inkan Layanan Migrasi Server untuk memigrasikan VM ke EC2: memungkinkan Layanan Migrasi Server menempatkan sumber daya yang dimigrasi ke akun EC2 pelanggan.

`ServerMigration_ServiceRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ServerMigration_ServiceRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 Agustus 2020, 20:41 UTC
- Waktu teredit: 15 Oktober 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*",
      "Condition" : {
```

```
        "Null" : {
          "cloudformation:ResourceTypes" : "false"
        },
        "ForAllValues:StringEquals" : {
          "cloudformation:ResourceTypes" : [
            "AWS::EC2::Instance",
            "AWS::ApplicationInsights::Application",
            "AWS::ResourceGroups::Group"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplate"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
```

```
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::sms-app-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sms:CreateReplicationJob",
        "sms:DeleteReplicationJob",
        "sms:GetReplicationJobs",
        "sms:GetReplicationRuns",
        "sms:GetServers",
        "sms:ImportServerCatalog",
        "sms:StartOnDemandReplicationRun",
        "sms:UpdateReplicationJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunRemoteScript",
        "arn:aws:s3:::sms-app-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/UseForSMSApplicationValidation" : [
            "true"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CopySnapshot"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CopySnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SMSJobId" : [
            "sms-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/SMSJobId" : [
            "sms-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CopyImage",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DeregisterImage",
        "ec2:ImportImage",
        "ec2:DescribeImportImageTasks",
        "ec2:GetEbsEncryptionByDefault"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetInstanceProfile"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "cloudformation.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ServerMigrationConnector

Deskripsi: Izin untuk mengizinkan Konektor Migrasi AWS Server untuk memigrasikan VM ke EC2. Memungkinkan komunikasi dengan Layanan Migrasi AWS Server, read/write akses ke bucket S3 dimulai dengan 'sms-b-' dan 'import-to-ec2-' serta bucket yang digunakan untuk peningkatan Konektor Migrasi AWS Server, pendaftaran Konektor Migrasi AWS Server dengan AWS, dan upload metrik ke. AWS

`ServerMigrationConnector`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ServerMigrationConnector` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Oktober 2016, 21:45 UTC
- Waktu teredit: 24 Oktober 2016, 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationConnector`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sms:SendMessage",
        "sms:GetMessages"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketLocation",
```

```
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutLifecycleConfiguration",
        "s3:AbortMultipartUpload",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "arn:aws:s3:::sms-b-*",
        "arn:aws:s3:::import-to-ec2-*",
        "arn:aws:s3:::server-migration-service-upgrade",
        "arn:aws:s3:::server-migration-service-upgrade/*",
        "arn:aws:s3:::connector-platform-upgrade-info/*",
        "arn:aws:s3:::connector-platform-upgrade-info",
        "arn:aws:s3:::connector-platform-upgrade-bundles/*",
        "arn:aws:s3:::connector-platform-upgrade-bundles",
        "arn:aws:s3:::connector-platform-release-notes/*",
        "arn:aws:s3:::connector-platform-release-notes"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "awsconnector:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ServerMigrationServiceConsoleFullAccess

Deskripsi: Izin yang diperlukan untuk menggunakan semua fitur Konsol Layanan Migrasi Server

`ServerMigrationServiceConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ServerMigrationServiceConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 Mei 2020, 17:18 UTC
- Waktu teredit: 20 Juli 2020, 22:00 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sms:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
```

```
    },
    {
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackResources"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "s3:ListAllMyBuckets",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Action" : [
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "sms.amazonaws.com"
```

```
        }
      },
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ServerMigrationServiceLaunchRole

Deskripsi: Izin untuk mengiz AWS inkan Layanan Migrasi Server membuat dan memperbarui AWS sumber daya yang relevan ke sumber daya pelanggan Akun AWS untuk meluncurkan server dan aplikasi yang dimigrasi.

`ServerMigrationServiceLaunchRole`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ServerMigrationServiceLaunchRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 November 2018, 19:53 UTC
- Waktu teredit: 15 Oktober 2020, 17:29 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute",
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
```

```
        "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:CreateApplication",
        "applicationinsights:CreateComponent",
        "applicationinsights:UpdateApplication",
```

```
        "applicationinsights:DeleteApplication",
        "applicationinsights:UpdateComponentConfiguration",
        "applicationinsights:DeleteComponent"
      ],
      "Resource" : "arn:aws:applicationinsights:*:*:application/resource-group/sms-app-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:GetGroup",
        "resource-groups:UpdateGroup",
        "resource-groups:DeleteGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/sms-app-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "application-insights.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ServerMigrationServiceRoleForInstanceValidation

Deskripsi: Izin untuk mengiz AWS inkan SMS menjalankan skrip validasi data yang digunakan dan mengirim skrip success/failure kembali ke SMS

`ServerMigrationServiceRoleForInstanceValidation`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ServerMigrationServiceRoleForInstanceValidation` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 Juli 2020, 22:25 UTC
- Waktu teredit: 20 Juli 2020, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sms:NotifyAppValidationOutput",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ServiceQuotasFullAccess

Deskripsi: Menyediakan akses penuh ke Kuota Layanan

`ServiceQuotasFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ServiceQuotasFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2019, 15:44 UTC

- Waktu teredit: 04 Februari 2021, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "cloudformation:DescribeAccountLimits",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "dynamodb:DescribeLimits",
        "elasticloadbalancing:DescribeAccountLimits",
        "iam:GetAccountSummary",
        "kinesis:DescribeLimits",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "rds:DescribeAccountAttributes",
        "route53:GetAccountLimit",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "servicequotas:*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/ServiceQuotaMonitor" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "servicequotas.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicequotas.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ServiceQuotasReadOnlyAccess

Deskripsi: Menyediakan akses baca saja ke Kuota Layanan

`ServiceQuotasReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ServiceQuotasReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Juni 2019, 15:31 UTC
- Waktu teredit: 12 Februari 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
```

```
        "cloudformation:DescribeAccountLimits",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "dynamodb:DescribeLimits",
        "elasticloadbalancing:DescribeAccountLimits",
        "iam:GetAccountSummary",
        "kinesis:DescribeLimits",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "rds:DescribeAccountAttributes",
        "route53:GetAccountLimit",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServices",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListTagsForResource",
        "servicequotas:GetAutoManagementConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:GetNotificationConfiguration",
        "notifications:GetEventRule",
        "notifications:ListNotificationHubs",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:GetEmailContact",
        "chatbot:ListMicrosoftTeamsChannelConfigurations",
        "chatbot:DescribeChimeWebhookConfigurations",
        "chatbot:DescribeSlackChannelConfigurations",
        "consoleapp:ListDeviceIdentities",
        "consoleapp:GetDeviceIdentity"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ServiceQuotasServiceRolePolicy

Deskripsi: Mengizinkan Kuota Layanan untuk membuat kasus dukungan atas nama Anda

`ServiceQuotasServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 22 Mei 2019, 20:44 UTC
- Waktu teredit: 24 Juni 2019, 14:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SignInLocalDevelopmentAccess

Deskripsi: Menyediakan izin untuk akses terprogram AWS melalui AWS Sign-in layanan, termasuk pembuatan token OAuth2 untuk alat dan aplikasi pengembang.

`SignInLocalDevelopmentAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SignInLocalDevelopmentAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 November 2025, 18:34 UTC
- Waktu teredit: 12 Februari 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/SignInLocalDevelopmentAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "signin:AuthorizeOAuth2Access",
        "signin:CreateOAuth2Token"
      ],
      "Resource" : "arn:aws:signin:*:*:oauth2/public-client/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SimpleWorkflowFullAccess

Deskripsi: Menyediakan akses penuh ke layanan konfigurasi Alur Kerja Sederhana.

`SimpleWorkflowFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SimpleWorkflowFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu teredit: 06 Februari 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/SimpleWorkflowFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "swf:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SMSVoiceServiceRolePolicy

Deskripsi: Mengizinkan SMSVoice mempublikasikan metrik CloudWatch atas nama Anda

`SMSVoiceServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 14 November 2024, 17:04 UTC
- Waktu teredit: 14 November 2024, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SMSVoiceServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/SMSVoice"
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SplitCostAllocationDataServiceRolePolicy

Deskripsi: Mengizinkan data alokasi biaya terpisah untuk mengambil informasi AWS Organisasi, jika berlaku, dan mengumpulkan data telemetri untuk layanan data alokasi biaya terpisah yang telah dipilih pelanggan.

`SplitCostAllocationDataServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 16 April 2024, 16:05 UTC
- Waktu teredit: 16 April 2024, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SplitCostAllocationDataServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListParents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonManagedServiceForPrometheusAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:ListWorkspaces",
        "aps:QueryMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SSMQuickSetupRolePolicy

Deskripsi: Memberikan izin untuk memeriksa kesehatan konfigurasi Pengaturan Cepat, memastikan penggunaan parameter dan sumber daya yang disediakan secara konsisten, dan memperbaiki sumber daya saat penyimpangan terdeteksi.

`SSMQuickSetupRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 25 Juni 2024, 15:20 UTC
- Waktu teredit: 18 November 2024, 13:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SSMQuickSetupRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SSMResourceDataSyncPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListResourceDataSync"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMResourceDataSyncGetOpsSummaryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsSummary"
      ],
      "Resource" : "arn:aws:ssm:*:*:resource-data-sync/AWS-QuickSetup-*"
```

```
    },
    {
      "Sid" : "SSMResourceDataSyncManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteResourceDataSync"
      ],
      "Resource" : "arn:aws:ssm:*:*:resource-data-sync/AWS-QuickSetup-*",
      "Condition" : {
        "StringEquals" : {
          "ssm:SyncType" : "SyncFromSource"
        }
      }
    },
    {
      "Sid" : "SSMAssociationsReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListAssociations",
        "ssm:DescribeAssociationExecutions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QuickSetupSSMDocumentsReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-*",
        "arn:aws:ssm:*:*:document/*-AWSQuickSetupType-*"
      ]
    },
    {
      "Sid" : "OrganizationReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAccountsForParent",
```

```
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedServicesForAccount"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QuickSetupStackSetReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults",
        "cloudformation:GetTemplate"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stackset/SSMQuickSetup*",
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SSMQuickSetup*"
      ]
    },
    {
      "Sid" : "QuickSetupStackSetDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStackInstances",
        "cloudformation:DeleteStackSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stackset/SSMQuickSetup*",
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SSMQuickSetup*",
        "arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stackset-target/SSMQuickSetup*",
        "arn:aws:cloudformation:*:*:type/resource/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "QuickSetupCfnStacksDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SupportUser

Deskripsi: Kebijakan ini memberikan izin untuk memecahkan masalah dan menyelesaikan masalah dalam Akun AWS. Kebijakan ini juga memungkinkan pengguna untuk menghubungi AWS dukungan untuk membuat dan mengelola kasus.

`SupportUser`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SupportUser` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan fungsi pekerjaan
- Waktu pembuatan: 10 November 2016, 17:21 UTC
- Waktu teredit: 12 Februari 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SupportUser`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*",
        "acm:DescribeCertificate",
        "acm:GetCertificate",
        "acm:List*",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities",
        "apigateway:GET",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:Describe*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:EstimateTemplateCost",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudsearch:Describe*",
        "cloudsearch:List*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents",
        "cloudtrail:ListTags",
        "cloudtrail:ListPublicKeys",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codecommit:BatchGetRepositories",
        "codecommit:Get*",
        "codecommit:List*",
```

```
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:AcknowledgeJob",
        "codepipeline:AcknowledgeThirdPartyJob",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:PollForJobs",
        "codepipeline:PollForThirdPartyJobs",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipeline",
        "cognito-identity:List*",
        "cognito-identity:LookupDeveloperIdentity",
        "cognito-identity:Describe*",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeRiskConfiguration",
        "cognito-idp:DescribeUserImportJob",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:List*",
        "cognito-sync:Describe*",
        "cognito-sync:GetBulkPublishDetails",
        "cognito-sync:GetCognitoEvents",
        "cognito-sync:GetIdentityPoolConfiguration",
        "cognito-sync:List*",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:DescribeConfigRules",
        "config:DescribeDeliveryChannels",
        "config:DescribeDeliveryChannelStatus",
        "config:GetResourceConfigHistory",
        "config:ListDiscoveredResources",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "datapipeline:ReportTaskProgress",
        "datapipeline:ReportTaskRunnerHeartbeat",
        "devicefarm:List*",
        "devicefarm:Get*",
        "directconnect:Describe*",
        "discovery:Describe*",
```

```
        "discovery:ListConfigurations",
        "dms:Describe*",
        "dms:List*",
        "ds:DescribeDirectories",
        "ds:DescribeSnapshots",
        "ds:GetDirectoryLimits",
        "ds:GetSnapshotLimits",
        "ds:ListAuthorizedApplications",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:Describe*",
        "ec2:DescribeHosts",
        "ec2:describeIdentityIdFormat",
        "ec2:DescribeIdFormat",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeNatGateways",
        "ec2:DescribeReservedInstancesModifications",
        "ec2:DescribeTags",
        "ec2:SearchLocalGatewayRoutes",
        "ecr:GetRepositoryPolicy",
        "ecr:BatchCheckLayerAvailability",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:Describe*",
        "ecs:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticbeanstalk:ValidateConfigurationSettings",
        "elasticfilesystem:Describe*",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elastictranscoder:List*",
        "elastictranscoder:ReadJob",
        "elasticfilesystem:DescribeFileSystems",
        "es:Describe*",
        "es:List*",
        "es:ESHttpGet",
```

```
        "es:ESHttpHead",
        "events:DescribeRule",
        "events:List*",
        "events:TestEventPattern",
        "firehose:Describe*",
        "firehose:List*",
        "gamelift:List*",
        "gamelift:Describe*",
        "glacier:ListVaults",
        "glacier:DescribeVault",
        "glacier:DescribeJob",
        "glacier:Get*",
        "glacier:List*",
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "importexport:GetStatus",
        "importexport:ListJobs",
        "inspector:Describe*",
        "inspector:List*",
        "iot:Describe*",
        "iot:Get*",
        "iot:List*",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:DiscoverInputSchema",
        "kinesisanalytics:GetApplicationState",
        "kinesisanalytics:ListApplications",
        "kinesis:Describe*",
        "kinesis:Get*",
        "kinesis:List*",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lambda:List*",
        "lambda:Get*",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "machinelearning:Describe*",
        "machinelearning:Get*",
        "opsworks:Describe*",
        "rds:Describe*",
        "rds:ListTagsForResource",
        "redshift:Describe*",
```

```
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53:Get*",
        "route53:List*",
        "route53domains:CheckDomainAvailability",
        "route53domains:GetDomainDetail",
        "route53domains:GetOperationDetail",
        "route53domains:List*",
        "s3:List*",
        "sdb:GetAttributes",
        "sdb:List*",
        "sdb:Select*",
        "servicecatalog:SearchProducts",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:ListLaunchPaths",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListRecordHistory",
        "servicecatalog:DescribeRecord",
        "servicecatalog:ScanProvisionedProducts",
        "ses:Get*",
        "ses:List*",
        "sns:Get*",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListQueues",
        "sqs:ReceiveMessage",
        "ssm:List*",
        "ssm:Describe*",
        "storagegateway:Describe*",
        "storagegateway:List*",
        "swf:Count*",
        "swf:Describe*",
        "swf:Get*",
        "swf:List*",
        "waf:Get*",
```

```
        "waf:List*",
        "workdocs:Describe*",
        "workmail:Describe*",
        "workmail:Get*",
        "workspaces:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

SystemAdministrator

Deskripsi: Memberikan izin akses penuh yang diperlukan untuk sumber daya yang diperlukan untuk operasi aplikasi dan pengembangan.

`SystemAdministrator`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `SystemAdministrator` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan fungsi pekerjaan
- Waktu pembuatan: 10 November 2016, 17:23 UTC
- Waktu teredit: 12 Februari 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SystemAdministrator`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Statement" : [
    {
      "Action" : [
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "acm:Request*",
        "acm:Resend*",
        "autoscaling:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListPublicKeys",
        "cloudtrail:ListTags",
        "cloudtrail:LookupEvents",
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudwatch:*",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateBranch",
        "codecommit:CreateRepository",
        "codecommit:Get*",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:List*",
        "codecommit:Put*",
        "codecommit:Test*",
        "codecommit:Update*",
        "codedeploy:*",
        "codepipeline:*",
        "config:*",
        "ds:*",
        "ec2:Allocate*",
```

```
        "ec2:AssignPrivateIpAddresses*",
        "ec2:Associate*",
        "ec2:Allocate*",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:Bundle*",
        "ec2:Cancel*",
        "ec2:Copy*",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDhcpOptions",
        "ec2:CreateFlowLogs",
        "ec2:CreateImage",
        "ec2:CreateInstanceExportTask",
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreatePlacementGroup",
        "ec2:CreateReservedInstancesListing",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateSpotDatafeedSubscription",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteKeyPair",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkInterface",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeleteSpotDatafeedSubscription",
```

```
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DeregisterImage",
        "ec2:Describe*",
        "ec2:DetachInternetGateway",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVolumeIO",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:GetConsoleOutput",
        "ec2:GetHostReservationPurchasePreview",
        "ec2:GetLaunchTemplateData",
        "ec2:GetPasswordData",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:Import*",
        "ec2:Modify*",
        "ec2:MonitorInstances",
        "ec2:MoveAddressToVpc",
        "ec2:Purchase*",
        "ec2:RegisterImage",
        "ec2:Release*",
        "ec2:Replace*",
        "ec2:ReportInstanceStatus",
        "ec2:Request*",
        "ec2:Reset*",
        "ec2:RestoreAddressToClassic",
        "ec2:RunScheduledInstances",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UnmonitorInstances",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
        "elasticloadbalancing:*",
        "events:*",
        "iam:GetAccount*",
```

```
        "iam:GetContextKeys*",
        "iam:GetCredentialReport",
        "iam:ListAccountAliases",
        "iam:ListGroups",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListPoliciesGrantingServiceAccess",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:Simulate*",
        "iam:UpdateServerCertificate",
        "iam:UpdateSigningCertificate",
        "kinesis:ListStreams",
        "kinesis:PutRecord",
        "kms:CreateAlias",
        "kms:CreateKey",
        "kms:DeleteAlias",
        "kms:Describe*",
        "kms:GenerateRandom",
        "kms:Get*",
        "kms:List*",
        "kms:Encrypt",
        "kms:ReEncrypt*",
        "lambda:Create*",
        "lambda:Delete*",
        "lambda:Get*",
        "lambda:InvokeFunction",
        "lambda:List*",
        "lambda:PublishVersion",
        "lambda:Update*",
        "logs:*",
        "rds:Describe*",
        "rds:ListTagsForResource",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "rolesanywhere:PutNotificationSettings",
```

```
        "rolesanywhere:ResetNotificationSettings",
        "route53:*",
        "route53domains:*",
        "ses:*",
        "sns:*",
        "sqs:*",
        "trustedadvisor:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AttachClassicLinkVpc",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateVpcPeeringConnection",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNetworkAcl*",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DetachClassicLinkVpc",
        "ec2:DetachVolume",
        "ec2:DisableVpcClassicLink",
        "ec2:EnableVpcClassicLink",
        "ec2:GetConsoleScreenshot",
        "ec2:RebootInstances",
        "ec2:RejectVpcPeeringConnection",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Effect" : "Allow",
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Action" : "s3:*",
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "iam:GetAccessKeyLastUsed",
        "iam:GetGroup*",
        "iam:GetInstanceProfile",
        "iam:GetLoginProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy*",
        "iam:GetRole*",
        "iam:GetSAMLProvider",
        "iam:GetSSHPublicKey",
        "iam:GetServerCertificate",
        "iam:GetServiceLastAccessed*",
        "iam:GetUser*",
        "iam:ListAccessKeys",
        "iam:ListAttached*",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles*",
        "iam:ListMFADevices",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListSSHPublicKeys",
        "iam:ListSigningCertificates",
        "iam:ListUserPolicies",
        "iam:Upload*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/rds-monitoring-role",
        "arn:aws:iam::*:role/ec2-sysadmin-*",
        "arn:aws:iam::*:role/ecr-sysadmin-*",
        "arn:aws:iam::*:role/lambda-sysadmin-*"
      ]
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

TranslateFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon Translate.

`TranslateFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `TranslateFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2018, 23:36 UTC
- Waktu teredit: 08 Januari 2020, 21:22 UTC

- ARN: `arn:aws:iam::aws:policy/TranslateFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "translate:*",
        "comprehend:DetectDominantLanguage",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

TranslateReadOnly

Deskripsi: Menyediakan akses baca-saja ke Amazon Translate.

`TranslateReadOnly`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `TranslateReadOnly` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2017, 18:22 UTC
- Waktu teredit: 24 Mei 2023, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateReadOnly`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "translate:TranslateText",
        "translate:TranslateDocument",
        "translate:GetTerminology",
        "translate:ListTerminologies",
        "translate:ListTextTranslationJobs",
        "translate:DescribeTextTranslationJob",
        "translate:GetParallelData",
```

```
        "translate:ListParallelData",
        "comprehend:DetectDominantLanguage",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

ViewOnlyAccess

Deskripsi: Kebijakan ini memberikan izin untuk melihat sumber daya dan metadata dasar di semua AWS layanan.

`ViewOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `ViewOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan fungsi pekerjaan
- Waktu pembuatan: 10 November 2016, 17:20 UTC
- Waktu teredit: 30 September 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/ViewOnlyAccess`

Versi kebijakan

Versi kebijakan: v46 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralViewOnlyAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "aiops:GetInvestigation",
        "aiops:GetInvestigationGroup",
        "aiops:ListInvestigationEvents",
        "aiops:ListInvestigationGroups",
        "aiops:ListInvestigations",
        "amplify:GetWebACLForResource",
        "amplify:ListDomainAssociations",
        "amplify:ListResourcesForWebACL",
        "apigateway:GetPortal",
        "apigateway:GetPortalProduct",
        "apigateway:GetPortalProductSharingPolicy",
        "apigateway:GetRoutingRule",
        "apigateway:ListPortalProducts",
        "apigateway:ListPortals",
        "apigateway:ListProductPages",
        "apigateway:ListProductRestEndpointPages",
        "apigateway:ListRoutingRules",
        "appconfig:GetAccountSettings",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExperimentDefinition",
        "appconfig:GetExtension",
        "appconfig:GetExtensionAssociation",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListDeployments",
```

```
        "appconfig:ListEnvironments",
        "appconfig:ListExperimentDefinitions",
        "appconfig:ListExperimentRuns",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListExtensions",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appsync:GetApi",
        "appsync:GetChannelNamespace",
        "appsync:GetGraphqlApi",
        "appsync:GetIntrospectionSchema",
        "appsync:GetResourcePolicy",
        "appsync:GetSourceApiAssociation",
        "athena:List*",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "backup:DescribeBackupJob",
        "backup:DescribeBackupVault",
        "backup:DescribeCopyJob",
        "backup:DescribeFramework",
        "backup:DescribeGlobalSettings",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeRegionSettings",
        "backup:DescribeReportJob",
        "backup:DescribeReportPlan",
        "backup:DescribeRestoreJob",
        "backup:GetBackupPlan",
        "backup:GetBackupPlanFromJSON",
        "backup:GetBackupPlanFromTemplate",
        "backup:GetBackupSelection",
        "backup:GetSupportedResourceTypes",
        "backup:ListBackupJobs",
        "backup:ListBackupPlans",
        "backup:ListBackupPlanTemplates",
        "backup:ListBackupPlanVersions",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListCopyJobs",
        "backup:ListFrameworks",
        "backup:ListLegalHolds",
        "backup:ListProtectedResources",
        "backup:ListProtectedResourcesByBackupVault",
        "backup:ListRecoveryPointsByBackupVault",
```

```
        "backup:ListRecoveryPointsByLegalHold",
        "backup:ListRecoveryPointsByResource",
        "backup:ListReportJobs",
        "backup:ListReportPlans",
        "backup:ListRestoreJobs",
        "backup:ListTags",
        "batch:ListJobs",
        "bedrock-agentcore:GetApiKeyCredentialProvider",
        "bedrock-agentcore:GetOauth2CredentialProvider",
        "bedrock-agentcore:GetResourcePolicy",
        "bedrock-agentcore:GetTokenVault",
        "bedrock-agentcore:ListApiKeyCredentialProviders",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "bedrock-agentcore:ListTagsForResource",
        "bedrock:GetAccountDataRetention",
        "bedrock:GetAdvancedPromptOptimizationJob",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:GetAsyncInvoke",
        "bedrock:GetAutomatedReasoningPolicy",
        "bedrock:GetAutomatedReasoningPolicyBuildWorkflow",
        "bedrock:GetAutomatedReasoningPolicyNextScenario",
        "bedrock:GetBlueprint",
        "bedrock:GetBlueprintOptimizationStatus",
        "bedrock:GetBlueprintRecommendation",
        "bedrock:GetCustomModel",
        "bedrock:GetCustomModelDeployment",
        "bedrock:GetDataAutomationLibrary",
        "bedrock:GetDataAutomationLibraryIngestionJob",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataAutomationStatus",
        "bedrock:GetDataSource",
        "bedrock:GetEvaluationJob",
        "bedrock:GetExecutionFlowSnapshot",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowExecution",
        "bedrock:GetFlowVersion",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
```

```
        "bedrock:GetGuardrail",
        "bedrock:GetImportedModel",
        "bedrock:GetInferenceProfile",
        "bedrock:GetIngestedDocumentAcl",
        "bedrock:GetIngestionJob",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetKnowledgeBaseDocuments",
        "bedrock:GetMarketplaceModelEndpoint",
        "bedrock:GetModelCopyJob",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationJob",
        "bedrock:GetResourcePolicy",
        "bedrock:ListCustomModels",
        "bedrock:ListTagsForResource",
        "clouddirectory:ListAppliedSchemaArns",
        "clouddirectory:ListDevelopmentSchemaArns",
        "clouddirectory:ListDirectories",
        "clouddirectory:ListPublishedSchemaArns",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplateSummary",
        "cloudformation:List*",
        "cloudfront:List*",
        "cloudsearch:DescribeDomains",
        "cloudsearch:List*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codeartifact:ListDomains",
        "codeartifact:ListPackages",
        "codebuild:ListBuilds*",
        "codebuild:ListProjects",
        "codecommit:List*",
        "codedeploy:BatchGetApplicationRevisions",
        "codedeploy:BatchGetApplications",
        "codedeploy:BatchGetDeploymentGroups",
        "codedeploy:BatchGetDeploymentInstances",
        "codedeploy:BatchGetDeployments",
        "codedeploy:BatchGetDeploymentTargets",
        "codedeploy:BatchGetOnPremisesInstances",
        "codedeploy:Get*",
        "codedeploy:List*",
```

```
        "codepipeline:ListPipelines",
        "codestar:List*",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentities",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:List*",
        "cognito-sync:ListDatasets",
        "comprehend:Describe*",
        "comprehend:List*",
        "config:Describe*",
        "config:List*",
        "connect:List*",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetAccountLimits",
        "datapipeline:ListPipelines",
        "dax:DescribeClusters",
        "dax:DescribeDefaultParameters",
        "dax:DescribeEvents",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "devicefarm:List*",
        "directconnect:Describe*",
        "discovery:List*",
        "dlm:GetLifecyclePolicies",
        "dlm:GetLifecyclePolicy",
        "dlm:ListTagsForResource",
        "dms:List*",
        "ds:DescribeDirectories",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeEndpoints",
        "dynamodb:DescribeExport",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
```

```
        "dynamodb:DescribeImport",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetAbacStatus",
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListBackups",
        "dynamodb:ListContributorInsights",
        "dynamodb:ListExports",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListImports",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAccountVpcEncryptionControl",
        "ec2:DescribeAddressTransfers",
        "ec2:DescribeAddresses",
        "ec2:DescribeAddressesAttribute",
        "ec2:DescribeAggregateIdFormat",
        "ec2:DescribeApplicationStatus",
        "ec2:DescribeApplicationStatusCheckAssociations",
        "ec2:DescribeApplicationStatusChecks",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAwsNetworkPerformanceMetricSubscriptions",
        "ec2:DescribeBundleTasks",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeCapacityBlockExtensionHistory",
        "ec2:DescribeCapacityBlockExtensionOfferings",
        "ec2:DescribeCapacityBlockOfferings",
        "ec2:DescribeCapacityBlockStatus",
        "ec2:DescribeCapacityBlocks",
        "ec2:DescribeCapacityManagerDataExports",
        "ec2:DescribeCapacityReservationBillingRequests",
        "ec2:DescribeCapacityReservationCancellationQuotes",
        "ec2:DescribeCapacityReservationFleets",
        "ec2:DescribeCapacityReservationTopology",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCarrierGateways",
```

```
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeClientVpnAuthorizationRules",
        "ec2:DescribeClientVpnConnections",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeClientVpnRoutes",
        "ec2:DescribeClientVpnTargetNetworks",
        "ec2:DescribeCoipPools",
        "ec2:DescribeConversionTasks",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDeclarativePoliciesReports",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeElasticGpus",
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeExportTasks",
        "ec2:DescribeFastLaunchImages",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DescribeFleetHistory",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeFpgaImageAttribute",
        "ec2:DescribeFpgaImages",
        "ec2:DescribeHost*",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeIdentityIdFormat",
        "ec2:DescribeIdFormat",
        "ec2:DescribeImage*",
        "ec2:DescribeImport*",
        "ec2:DescribeInstance*",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamByoasn",
        "ec2:DescribeIpamExternalResourceVerificationTokens",
        "ec2:DescribeIpamInternetRegistryAssociations",
        "ec2:DescribeIpamPolicies",
        "ec2:DescribeIpamPoolAllocations",
        "ec2:DescribeIpamPools",
        "ec2:DescribeIpamPrefixListResolverTargets",
        "ec2:DescribeIpamPrefixListResolvers",
        "ec2:DescribeIpamResourceDiscoveries",
        "ec2:DescribeIpamResourceDiscoveryAssociations",
        "ec2:DescribeIpamScopes",
        "ec2:DescribeIpams",
        "ec2:DescribeIpv6Pools",
```

```
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeLockedSnapshots",
        "ec2:DescribeMacHosts",
        "ec2:DescribeMacModificationTasks",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetwork*",
        "ec2:DescribeOutpostLags",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePrefixLists",
        "ec2:DescribePrincipalIdFormat",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeRegions",
        "ec2:DescribeReplaceRootVolumeTasks",
        "ec2:DescribeReserved*",
        "ec2:DescribeRouteServerEndpoints",
        "ec2:DescribeRouteServerPeers",
        "ec2:DescribeRouteServers",
        "ec2:DescribeRouteTables",
        "ec2:DescribeScheduledInstanceAvailability",
        "ec2:DescribeScheduledInstances",
        "ec2:DescribeSecondaryInterfaces",
        "ec2:DescribeSecondaryNetworks",
        "ec2:DescribeSecondarySubnets",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeServiceLinkVirtualInterfaces",
        "ec2:DescribeSnapshot*",
        "ec2:DescribeSpot*",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeStoreImageTasks",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilterRules",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayMeteringPolicies",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:DescribeTransitGatewayRouteTableAnnouncements",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTrunkInterfaceAssociations",
        "ec2:DescribeVerifiedAccessEndpoints",
        "ec2:DescribeVerifiedAccessGroups",
        "ec2:DescribeVerifiedAccessInstanceLoggingConfigurations",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessTrustProviders",
        "ec2:DescribeVolume*",
        "ec2:DescribeVpc*",
        "ec2:DescribeVpnConcentrators",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetActiveVpnTunnelStatus",
        "ec2:GetAllowedImagesSettings",
        "ec2:GetAssociatedEnclaveCertificateIamRoles",
        "ec2:GetAssociatedIpv6PoolCidrs",
        "ec2:GetCapacityManagerAttributes",
        "ec2:GetCapacityManagerMetricDimensions",
        "ec2:GetCapacityManagerMonitoredTagKeys",
        "ec2:GetCapacityReservationUsage",
        "ec2:GetCoipPoolUsage",
        "ec2:GetDeclarativePoliciesReportSummary",
        "ec2:GetDefaultCreditSpecification",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEnabledIpamPolicy",
        "ec2:GetFlowLogsIntegrationTemplate",
        "ec2:GetGroupsForCapacityReservation",
```

```
        "ec2:GetHostReservationPurchasePreview",
        "ec2:GetImageAncestry",
        "ec2:GetImageBlockPublicAccessState",
        "ec2:GetInstanceMetadataDefaults",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamAddressHistory",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "ec2:GetIpamDiscoveredRoutes",
        "ec2:GetIpamInternetRegistryAssociationAsns",
        "ec2:GetIpamInternetRegistryAssociationCidrs",
        "ec2:GetIpamPolicyAllocationRules",
        "ec2:GetIpamPolicyOrganizationTargets",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetIpamPrefixListResolverRules",
        "ec2:GetIpamPrefixListResolverVersions",
        "ec2:GetIpamResourceCidrs",
        "ec2:GetIpamRouteOriginAuthorizations",
        "ec2:GetIpamRouteProtectionFindings",
        "ec2:GetIpamRoutingPolicyRegistrations",
        "ec2:GetManagedPrefixListAssociations",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetManagedResourceVisibility",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetReservedInstancesExchangeQuote",
        "ec2:GetResourcePolicy",
        "ec2:GetRouteServerAssociations",
        "ec2:GetRouteServerPropagations",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:GetSerialConsoleAccessStatus",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetSpotPlacementScores",
        "ec2:GetSubnetCidrReservations",
        "ec2:GetTransitGatewayAttachmentPropagations",
        "ec2:GetTransitGatewayMeteringPolicyEntries",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayPolicyTableAssociations",
        "ec2:GetTransitGatewayPolicyTableEntries",
        "ec2:GetTransitGatewayPrefixListReferences",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessEndpointTargets",
```

```
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:GetVpcResourcesBlockingEncryptionEnforcement",
        "ec2:GetVpnConnectionDeviceTypes",
        "ec2:GetVpnTunnelReplacementStatus",
        "ec2:ListImagesInRecycleBin",
        "ec2:ListSnapshotsInRecycleBin",
        "ec2:ListVolumesInRecycleBin",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:SearchTransitGatewayRoutes",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:Describe*",
        "ecs:List*",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeAddonConfiguration",
        "eks:DescribeAddonVersions",
        "eks:DescribeCapability",
        "eks:DescribeCluster",
        "eks:DescribeClusterVersions",
        "eks:DescribeEksAnywhereSubscription",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeInsight",
        "eks:DescribeInsightsRefresh",
        "eks:DescribeNodegroup",
        "eks:DescribePodIdentityAssociation",
        "eks:DescribeUpdate",
        "eks:ListAccessEntries",
        "eks:ListAccessPolicies",
        "eks:ListAddons",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListCapabilities",
        "eks:ListClusters",
        "eks:ListEksAnywhereSubscriptions",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListInsights",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "eks:ListTagsForResource",
```

```
        "eks:ListUpdates",
        "elasticache:Describe*",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeApplicationVersions",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticbeanstalk:ListAvailableSolutionStacks",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:List*",
        "elastictranscoder:List*",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:ListApplications",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:ListDomainNames",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "firehose:DescribeDeliveryStream",
        "firehose:List*",
        "fsx:DescribeFileSystems",
        "gamelift:List*",
        "glacier:DescribeJob",
        "glacier:GetVaultAccessPolicy",
        "glacier:GetVaultNotifications",
        "glacier:List*",
        "glue:GetJobRuns",
        "glue:GetResourcePolicies",
        "glue:GetSchema",
        "glue:GetTable",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:GetTags",
        "glue:ListJobs",
        "glue:ListSchemaVersions",
        "glue:ListSchemas",
        "glue:ListSessions",
```

```
        "greengrass:List*",
        "iam:GetAccountSummary",
        "iam:GetLoginProfile",
        "iam:List*",
        "importexport:ListJobs",
        "inspector:List*",
        "iot:List*",
        "kafka:ListClusters",
        "kendra:ListDataSources",
        "kendra:ListTagsForResource",
        "kinesis:ListStreams",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetResourcePolicy",
        "lambda:List*",
        "lex:GetBotAliases",
        "lex:GetBotChannelAssociations",
        "lex:GetBots",
        "lex:GetBotVersions",
        "lex:GetIntents",
        "lex:GetIntentVersions",
        "lex:GetSlotTypes",
        "lex:GetSlotTypeVersions",
        "lex:GetUtterancesView",
        "lightsail:GetBlueprints",
        "lightsail:GetBundles",
        "lightsail:GetInstances",
        "lightsail:GetInstancePortStates",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetKeyPair",
        "lightsail:GetRegions",
        "lightsail:GetStaticIps",
        "lightsail:IsVpcPeered",
        "logs:Describe*",
        "logs:GetTransformer",
        "logs:ListEntitiesForLogGroup",
        "logs:ListLogGroupsForEntity",
        "logs:ListLogGroupsForQuery",
        "logs:ListTagsForResource",
        "lookoutvision:ListModelPackagingJobs",
```

```
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:ListApplications",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "machinelearning:Describe*",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mediaconnect:ListRouterInputs",
        "mediaconnect:ListRouterOutputs",
        "mediaconnect:ListRouterNetworkInterfaces",
        "mediastore:DescribeContainer",
        "mediastore:GetLifecyclePolicy",
        "mediastore:ListTagsForResource",
        "memorydb:DescribeAcls",
        "memorydb:DescribeUsers",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetImportJobs",
        "mobiletargeting:GetSegments",
        "oam:ListAttachedLinks",
        "oam:ListLinks",
        "oam:ListSinks",
        "opsworks-cm:Describe*",
        "opsworks:Describe*",
        "organizations:List*",
        "outposts:GetOutpost",
        "outposts:GetOutpostInstanceTypes",
        "outposts:ListOutposts",
        "outposts:ListSites",
        "outposts:ListTagsForResource",
        "polly:Describe*",
        "polly:List*",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "qapps:GetQApp",
        "qapps:ListQApps",
        "qapps:ListTagsForResource",
        "qbusiness:GetApplication",
        "qbusiness:GetDataSource",
```

```
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetPolicy",
        "qbusiness:GetRetriever",
        "qbusiness:GetWebExperience",
        "ram:GetResourceShareAssociations",
        "rds:Describe*",
        "redshift-serverless:GetResourcePolicy",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusters",
        "redshift:DescribeEvents",
        "redshift:ViewQueriesInConsole",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53:Get*",
        "route53:List*",
        "route53domains:List*",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sdb:List*",
        "servicecatalog:List*",
```

```
        "ses:DescribeActiveReceiptRuleSet",
        "ses:List*",
        "ses:ListDedicatedIpPools",
        "shield:List*",
        "sns:GetDataProtectionPolicy",
        "sns:GetSubscriptionAttributes",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListMessageMoveTasks",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "states:ListActivities",
        "states:ListExecutions",
        "states:ListMapRuns",
        "states:ListStateMachineAliases",
        "states:ListStateMachines",
        "states:ListStateMachineVersions",
        "storagegateway:DescribeSMBSettings",
        "storagegateway:ListGateways",
        "storagegateway:ListLocalDisks",
        "storagegateway:ListVolumeRecoveryPoints",
        "storagegateway:ListVolumes",
        "swf:List*",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts",
        "trustedadvisor:Describe*",
        "uxc:GetAccountCustomizations",
        "uxc:ListServices",
        "waf-regional:List*",
        "waf:List*",
        "wafv2:List*",
        "wisdom:ListAssistants",
        "workdocs:DescribeAvailableDirectories",
        "workdocs:DescribeInstances",
        "workmail:Describe*",
        "workspaces:Describe*",
        "xray:GetEncryptionConfig",
        "xray:GetGroups",
        "xray:GetSamplingRules",
```

```
        "xray:GetSamplingStatisticSummaries",
        "xray:GetSamplingTargets",
        "xray:GetTraceSegmentDestination",
        "xray:ListResourcePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/cors",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/exports/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses/*",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses",
```

```
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/tags/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

VMImportExportRoleForAWSConnector

Deskripsi: Kebijakan default untuk peran Import/Export layanan VM, untuk pelanggan yang menggunakan AWS Konektor. Import/Export Layanan VM mengambil peran dengan kebijakan ini untuk memenuhi permintaan migrasi mesin virtual dari alat virtual AWS Connector. (Perhatikan bahwa AWS Konektor menggunakan kebijakan terkelola “AWSConnector” untuk mengeluarkan permintaan atas nama pelanggan ke Import/Export layanan VM.) Menyediakan kemampuan untuk membuat AMI dan snapshot EBS, memodifikasi atribut snapshot EBS, melakukan panggilan “Deskribe*” pada objek EC2, dan membaca dari bucket S3 dimulai dengan 'import-to-ec2'.

`VMImportExportRoleForAWSConnector`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `VMImportExportRoleForAWSConnector` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 03 September 2015, 20:48 UTC
- Waktu teredit: 03 September 2015, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::import-to-ec2-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:CopySnapshot",
        "ec2:RegisterImage",
        "ec2:Describe*"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

VPCLatticeFullAccess

Deskripsi: Menyediakan akses penuh ke Amazon VPC Lattice dan akses ke layanan ketergantungan.

`VPCLatticeFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `VPCLatticeFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Maret 2023, 02:49 UTC
- Waktu teredit: 12 Februari 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "logs:DescribeLogGroups",
        "s3:ListAllMyBuckets",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:UpdateLogDelivery",
        "logs:DescribeResourcePolicies"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "vpc-lattice.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "vpc-lattice.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "delivery.logs.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

VPCLatticeReadOnlyAccess

Deskripsi: Menyediakan akses baca-saja ke Amazon VPC Lattice melalui Konsol Manajemen AWS, dan akses terbatas ke layanan ketergantungan.

`VPCLatticeReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `VPCLatticeReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: Maret 30, 2023, 02:47 UTC
- Waktu teredit: 12 Februari 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:Get*",
        "vpc-lattice:List*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction",
        "logs:DescribeLogGroups",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "s3:ListAllMyBuckets",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

VPCLatticeServicesInvokeAccess

Deskripsi: Menyediakan akses untuk memanggil layanan Amazon VPC Lattice.

`VPCLatticeServicesInvokeAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `VPCLatticeServicesInvokeAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: Maret 30, 2023, 02:45 UTC
- Waktu teredit: 30 Maret 2023, 02:45 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice-svcs:Invoke"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

WAFLoggingServiceRolePolicy

Deskripsi: Membuat SLR untuk menulis log pelanggan ke aliran firehose

`WAFLoggingServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 24 Agustus 2018, 21:05 UTC
- Waktu teredit: 20 Mei 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "KMSForFirehoseSSECMK",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "firehose.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

WAFRegionalLoggingServiceRolePolicy

Deskripsi: Membuat SLR untuk menulis log pelanggan ke aliran firehose

`WAFRegionalLoggingServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 24 Agustus 2018, 18:40 UTC
- Waktu yang diedit: 20 Mei 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    },
```

```
    {
      "Sid" : "KMSForFirehoseSSECMK",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "firehose.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

WAFV2LoggingServiceRolePolicy

Deskripsi: Kebijakan ini membuat peran terkait layanan yang memungkinkan AWS WAF menulis log ke Amazon Kinesis Data Firehose.

`WAFV2LoggingServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Detail kebijakan

- Jenis: kebijakan Service-linked peran
- Waktu pembuatan: 07 November 2019, 00:40 UTC
- Waktu yang diedit: 20 Mei 2026, 18:12 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FirehoseAPIStatement",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "DescribeOrganizationAPIStatement",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSForFirehoseSSECMK",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "kms:ViaService" : "firehose.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

WellArchitectedAgentResourceScanning

Deskripsi: Memberikan akses read-only kepada AWS Well-Architected Agen ke konfigurasi AWS sumber daya, pengaturan keamanan, dan data operasional untuk menghasilkan rekomendasi pengoptimalan

`WellArchitectedAgentResourceScanning`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `WellArchitectedAgentResourceScanning` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 16 Juli 2026, 20:27 UTC
- Waktu teredit: 30 September 2026, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedAgentResourceScanning`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudControlDiscoveryCompact",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:List*",
        "acm-pca:Describe*",
        "acm-pca:Get*",
        "acm-pca:List*",
        "acm:DescribeCertificate",
        "aco-automation:GetAutomationRule",
        "aco-automation:ListAutomationRules",
        "aidevops:DescribePrivateConnection",
        "aidevops:Get*",
        "aidevops:List*",
        "aiops:Get*",
        "aiops:List*",
        "airflow-serverless:GetWorkflow",
        "airflow-serverless:List*",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "amplify:Get*",
        "amplify:List*",
        "amplifyuibuilder:Get*",
        "amplifyuibuilder:List*",
        "apigateway:GetRoutingRule",
        "apigateway:ListRoutingRules",
        "app-integrations:Get*",
        "app-integrations:List*",
        "appconfig:Get*",
        "appconfig:List*",
        "appflow:Describe*",
        "appflow:List*",
        "application-autoscaling:Describe*",
```

```
        "application-signals:GetServiceLevelObjective",
        "application-signals:List*",
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "apprunner:Describe*",
        "apprunner:List*",
        "appstream:Describe*",
        "appstream:List*",
        "apptest:GetTestCase",
        "apptest:List*",
        "aps:Describe*",
        "aps:List*",
        "arc-region-switch:GetPlan",
        "arc-region-switch:List*",
        "arc-zonal-shift:Get*",
        "arc-zonal-shift:ListManagedResources",
        "athena:Get*",
        "athena:List*",
        "auditmanager:GetAssessment",
        "auditmanager:List*",
        "autoscaling:Describe*",
        "aws-external-anthropic:GetWorkspace",
        "aws-external-anthropic:List*",
        "b2bi:Get*",
        "b2bi:List*",
        "backup-gateway:GetHypervisor",
        "backup-gateway:List*",
        "backup:Describe*",
        "backup:Get*",
        "backup:List*",
        "batch:Describe*",
        "batch:List*",
        "bcm-data-exports:GetExport",
        "bcm-data-exports:List*",
        "bcm-pricing-calculator:GetBillScenario",
        "bcm-pricing-calculator:List*",
        "bedrock-agentcore:Get*",
        "bedrock-agentcore:List*",
        "bedrock-mantle:GetProject",
        "bedrock-mantle:List*",
        "bedrock:Get*",
        "bedrock:List*",
        "billing:GetBillingView",
        "billing:List*",
```

```
        "billingconductor:List*",
        "braket:ListTagsForResource",
        "braket:Search*",
        "budgets:Describe*",
        "budgets:ListTagsForResource",
        "ce:DescribeCostCategoryDefinition",
        "ce:Get*",
        "ce:GetCostAndUsage",
        "ce:GetCostAndUsageWithResources",
        "ce:List*",
        "chatbot:Describe*",
        "chatbot:Get*",
        "chatbot:List*",
        "chime:Describe*",
        "chime:List*",
        "cleanrooms-ml:Get*",
        "cleanrooms-ml:List*",
        "cleanrooms:Get*",
        "cleanrooms:List*",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:ListResources",
        "cloudformation:ListTypes",
        "cloudfront:Describe*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudtrail:Describe*",
        "cloudtrail:Get*",
        "cloudtrail:List*",
        "cloudwatch:Describe*",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:Get*",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricWidgetImage",
        "cloudwatch:List*",
        "cloudwatch:ListMetrics",
        "codeartifact:Describe*",
        "codeartifact:Get*",
        "codeartifact:List*",
        "codebuild:BatchGetFleets",
        "codebuild:ListFleets",
        "codecommit:Get*",
        "codeconnections:GetConnection",
```

```
        "codeconnections:List*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:Get*",
        "codeguru-profiler:List*",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:List*",
        "codepipeline:Get*",
        "codepipeline:List*",
        "codestar-connections:Get*",
        "codestar-connections:List*",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:ListNotificationRules",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:Get*",
        "cognito-identity:ListIdentityPools",
        "comprehend:Describe*",
        "comprehend:List*",
        "config:Describe*",
        "config:GetStoredQuery",
        "config:List*",
        "connect-campaigns:Describe*",
        "connect-campaigns:List*",
        "controltower:Get*",
        "controltower:List*",
        "cur:Describe*",
        "cur:ListTagsForResource",
        "databrew:Describe*",
        "databrew:List*",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datasync:Describe*",
        "datasync:List*",
        "deadline:Get*",
        "deadline:List*",
        "detective:Describe*",
        "detective:GetMembers",
        "detective:List*",
        "devicefarm:Get*",
        "devicefarm:List*",
        "devops-guru:Describe*",
        "devops-guru:Get*",
```

```
        "devops-guru:List*",
        "directconnect:Describe*",
        "dms:Describe*",
        "dms:List*",
        "ds:Describe*",
        "ds:ListTagsForResource",
        "dsql:Get*",
        "dsql:List*",
        "ecr-public:Describe*",
        "ecr-public:Get*",
        "ecr-public:ListTagsForResource",
        "ecr:Describe*",
        "ecr:Get*",
        "ecr:List*",
        "ecs:Describe*",
        "ecs:List*",
        "eks:Describe*",
        "eks:List*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticfilesystem:Describe*",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:List*",
        "elemental-inference:GetFeed",
        "elemental-inference:List*",
        "emr-containers:Describe*",
        "emr-containers:List*",
        "emr-serverless:GetApplication",
        "emr-serverless:ListApplications",
        "entityresolution:Get*",
        "entityresolution:List*",
        "events:Describe*",
        "events:List*",
        "evidently:GetSegment",
        "evidently:List*",
        "evs:GetEnvironment",
        "evs:List*",
        "finspace:GetEnvironment",
        "finspace:ListEnvironments",
        "firehose:DescribeDeliveryStream",
        "firehose:List*",
        "fis:Get*",
```

```
        "fis:List*",
        "fms:Get*",
        "fms:List*",
        "forecast:Describe*",
        "forecast:List*",
        "fsx:Describe*",
        "gamelift:Describe*",
        "gamelift:List*",
        "gamelift:ValidateMatchmakingRuleSet",
        "gameliftstreams:Get*",
        "gameliftstreams:List*",
        "geo:Describe*",
        "geo:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "grafana:Describe*",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetDeployment",
        "greengrass:List*",
        "groundstation:Get*",
        "groundstation:List*",
        "guardduty:DescribePublishingDestination",
        "guardduty:Get*",
        "guardduty:List*",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:List*",
        "iam:Get*",
        "iam:List*",
        "imagebuilder:Get*",
        "imagebuilder:List*",
        "inspector:Describe*",
        "inspector:List*",
        "inspector2:Get*",
        "inspector2:List*",
        "interconnect:GetConnection",
        "interconnect:List*",
        "internetmonitor:Get*",
        "internetmonitor:List*",
        "invoicing:GetInvoiceUnit",
        "invoicing:List*",
        "iot:Describe*",
        "iot:Get*",
        "iot:List*",
```

```
        "iotanalytics:Describe*",
        "iotanalytics:List*",
        "iotdeviceadvisor:GetSuiteDefinition",
        "iotdeviceadvisor:ListSuiteDefinitions",
        "iotevents:Describe*",
        "iotevents:List*",
        "iotfleetwise:Get*",
        "iotfleetwise:List*",
        "iotsitewise:Describe*",
        "iotsitewise:List*",
        "iottwinmaker:Get*",
        "iottwinmaker:List*",
        "iotwireless:Get*",
        "iotwireless:List*",
        "ivs:Get*",
        "ivs:List*",
        "ivschat:Get*",
        "ivschat:List*",
        "kafka-cluster:Describe*",
        "kafka:Describe*",
        "kafka:Get*",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kendra-ranking:DescribeRescoreExecutionPlan",
        "kendra-ranking:List*",
        "kendra:Describe*",
        "kendra:List*",
        "kinesis:Describe*",
        "kinesis:List*",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kinesisvideo:List*",
        "lakeformation:Describe*",
        "lakeformation:GetLFTag",
        "lakeformation:List*",
        "lambda:GetFunctionConcurrency",
        "launchwizard:GetDeployment",
        "launchwizard:List*",
        "lex:Describe*",
        "lex:GetBotAlias",
        "lex:List*",
        "license-manager:Get*",
```

```
        "license-manager:List*",
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListInferenceSchedulers",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:Get*",
        "m2:List*",
        "macie2:Get*",
        "macie2:List*",
        "managedblockchain:GetAccessor",
        "managedblockchain:ListAccessors",
        "mediaconnect:Describe*",
        "mediaconnect:Get*",
        "mediaconnect:List*",
        "medialive:Describe*",
        "medialive:Get*",
        "medialive:List*",
        "mediapackage-vod:Describe*",
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:Get*",
        "mediapackagev2:List*",
        "mediatailor:Describe*",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:List*",
        "medical-imaging:GetDatastore",
        "medical-imaging:List*",
        "mobiletargeting:Get*",
        "mobiletargeting:List*",
        "mpa:Get*",
        "mpa:List*",
        "mq:Describe*",
        "mq:List*",
        "network-firewall:Describe*",
        "network-firewall:List*",
        "networkmanager:Describe*",
        "networkmanager:Get*",
        "networkmanager:List*",
        "nimble:GetStudio",
        "nimble:ListStudios",
```

```
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:List*",
        "notifications:Get*",
        "notifications:List*",
        "nova-act:GetWorkflowDefinition",
        "nova-act:ListWorkflowDefinitions",
        "oam:Get*",
        "oam:List*",
        "observabilityadmin:Get*",
        "observabilityadmin:List*",
        "odb:Get*",
        "odb:List*",
        "omics:Get*",
        "omics:List*",
        "organizations:Describe*",
        "organizations:List*",
        "osis:Get*",
        "osis:List*",
        "panorama:Describe*",
        "panorama:List*",
        "payment-cryptography:Get*",
        "payment-cryptography:List*",
        "pca-connector-ad:Get*",
        "pca-connector-ad:List*",
        "pca-connector-scep:Get*",
        "pca-connector-scep:List*",
        "pcs:Get*",
        "pcs:List*",
        "personalize:Describe*",
        "personalize:List*",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "profile:Get*",
        "profile:List*",
        "proton:Get*",
        "proton:List*",
        "qbusiness:Get*",
        "qbusiness:List*",
        "quicksight:Describe*",
        "quicksight:List*",
        "ram:Get*",
        "ram:List*",
        "rbin:GetRule",
        "rbin:List*",
```

```
        "refactor-spaces:Get*",
        "refactor-spaces:List*",
        "rekognition:Describe*",
        "rekognition:List*",
        "resiliencehub:Describe*",
        "resiliencehub:Get*",
        "resiliencehub:List*",
        "resource-explorer-2:Get*",
        "resource-explorer-2:List*",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:SearchResources",
        "robomaker:Describe*",
        "robomaker:List*",
        "rolesanywhere:Get*",
        "rolesanywhere:List*",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:Get*",
        "route53-recovery-readiness:List*",
        "route53:Get*",
        "route53:List*",
        "route53profiles:Get*",
        "route53profiles:List*",
        "route53resolver:Get*",
        "route53resolver:List*",
        "rtbfabric:Get*",
        "rtbfabric:List*",
        "rum:BatchGetRumMetricDefinitions",
        "rum:Get*",
        "rum:List*",
        "sagemaker:Describe*",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:List*",
        "sagemaker:ListMonitoringSchedules",
        "scheduler:Get*",
        "scheduler:List*",
        "schemas:Describe*",
        "schemas:List*",
        "securitylake:Get*",
        "securitylake:List*",
        "servicecatalog:Describe*",
        "servicecatalog:Get*",
        "servicecatalog:List*",
```

```
        "ses:Describe*",
        "ses:Get*",
        "ses:List*",
        "shield:Describe*",
        "shield:List*",
        "signer:Get*",
        "signer:List*",
        "simspaceweaver:DescribeSimulation",
        "simspaceweaver:ListSimulations",
        "sms-voice:Describe*",
        "sms-voice:Get*",
        "sms-voice:List*",
        "sns:Get*",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:List*",
        "ssm-contacts:Get*",
        "ssm-contacts:List*",
        "ssm-guiconnect:Get*",
        "ssm-incidents:Get*",
        "ssm-incidents:List*",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-sap:GetApplication",
        "ssm-sap:List*",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "states:Describe*",
        "states:List*",
        "supportapp:Get*",
        "supportapp:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "tag:GetResources",
        "thinclient:GetEnvironment",
        "thinclient:List*",
        "transfer:Describe*",
        "transfer:List*",
        "trustedadvisor:GetRecommendation",
        "trustedadvisor:ListChecks",
        "trustedadvisor:ListRecommendationResources",
        "trustedadvisor:ListRecommendations",
```

```
        "trustedadvisor:ListRecommendationsForResource",
        "verifiedpermissions:Get*",
        "verifiedpermissions:List*",
        "voiceid:DescribeDomain",
        "voiceid:List*",
        "vpc-lattice:Get*",
        "vpc-lattice:List*",
        "wafv2:Get*",
        "wafv2:List*",
        "wisdom:Get*",
        "wisdom:List*",
        "workspaces-instances:Get*",
        "workspaces-instances:List*",
        "workspaces-web:Get*",
        "workspaces-web:List*",
        "workspaces:Describe*",
        "xray:Get*",
        "xray:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudControlDiscoveryCompactExact",
      "Effect" : "Allow",
      "Action" : [
        "aoss:BatchGetCollection",
        "aoss:BatchGetCollectionGroup",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollectionGroups",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListTagsForResource",
        "aoss:ListVpcEndpoints",
        "appsync:GetApi",
        "appsync:GetChannelNamespace",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
```

```
        "appsync:GetGraphqlApi",
        "appsync:GetSourceApiAssociation",
        "appsync:ListApis",
        "appsync:ListChannelNamespaces",
        "appsync:ListDataSources",
        "appsync:ListDomainNames",
        "appsync:ListFunctions",
        "appsync:ListGraphqlApis",
        "appsync:ListResolvers",
        "appsync:ListSourceApiAssociations",
        "appsync:ListTagsForResource",
        "cases:BatchGetCaseRule",
        "cases:BatchGetField",
        "cases:GetDomain",
        "cases:GetLayout",
        "cases:GetTemplate",
        "cases:ListCaseRules",
        "cases:ListDomains",
        "cases:ListFields",
        "cases:ListLayouts",
        "cases:ListTemplates",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:DescribePublisher",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeType",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
        "cloudformation:ListTypes",
        "cloudformation:ListTypeVersions",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeTerms",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:GetGroup",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
```

```
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTerms",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "connect:DescribeAgentStatus",
        "connect:DescribeContactFlow",
        "connect:DescribeContactFlowModule",
        "connect:DescribeContactFlowModuleAlias",
        "connect:DescribeDataTable",
        "connect:DescribeEvaluationForm",
        "connect:DescribeHoursOfOperation",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribeNotification",
        "connect:DescribePhoneNumber",
        "connect:DescribePredefinedAttribute",
        "connect:DescribePrompt",
        "connect:DescribeQueue",
        "connect:DescribeQuickConnect",
        "connect:DescribeRoutingProfile",
        "connect:DescribeRule",
        "connect:DescribeSecurityProfile",
        "connect:DescribeTrafficDistributionGroup",
        "connect:DescribeUserHierarchyGroup",
        "connect:DescribeView",
        "connect:DescribeWorkspace",
        "connect:GetTaskTemplate",
        "connect:ListAgentStatuses",
        "connect:ListApprovedOrigins",
        "connect:ListBots",
        "connect:ListContactFlowModuleAliases",
        "connect:ListContactFlowModules",
        "connect:ListContactFlowModuleVersions",
        "connect:ListContactFlows",
        "connect:ListContactFlowVersions",
        "connect:ListDataTableAttributes",
        "connect:ListDataTables",
        "connect:ListEvaluationForms",
        "connect:ListEvaluationFormVersions",
        "connect:ListHoursOfOperationOverrides",
        "connect:ListHoursOfOperations",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
```

```
        "connect:ListIntegrationAssociations",
        "connect:ListLambdaFunctions",
        "connect:ListNotifications",
        "connect:ListPredefinedAttributes",
        "connect:ListPrompts",
        "connect:ListQueueEmailAddresses",
        "connect:ListQueueQuickConnects",
        "connect:ListQueues",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileManualAssignmentQueues",
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListSecurityProfileApplications",
        "connect:ListSecurityProfileFlowModules",
        "connect:ListSecurityProfilePermissions",
        "connect:ListSecurityProfiles",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListTrafficDistributionGroups",
        "connect:ListUserHierarchyGroups",
        "connect:ListUserProficiencies",
        "connect:ListUsers",
        "connect:ListViews",
        "connect:ListViewVersions",
        "connect:ListWorkspaceMedia",
        "connect:ListWorkspacePages",
        "connect:ListWorkspaces",
        "connect:SearchWorkspaceAssociations",
        "datazone:GetDataSource",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentProfile",
        "datazone:GetGroupProfile",
        "datazone:GetProject",
        "datazone:GetProjectProfile",
        "datazone:GetSubscriptionTarget",
        "datazone:GetUserProfile",
        "datazone:ListConnections",
        "datazone:ListDataSources",
```

```
        "datazone:ListDomains",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjectProfiles",
        "datazone:ListProjects",
        "datazone:ListSubscriptionTargets",
        "datazone:SearchGroupProfiles",
        "datazone:SearchUserProfiles",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAwsNetworkPerformanceMetricSubscriptions",
        "ec2:DescribeCapacityManagerDataExports",
        "ec2:DescribeCapacityReservationFleets",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeHosts",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceConnectEndpoints",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeInstances",
```

```
        "ec2:DescribeInstanceSqlHaStates",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamPools",
        "ec2:DescribeIpamPrefixListResolvers",
        "ec2:DescribeIpamPrefixListResolverTargets",
        "ec2:DescribeIpamResourceDiscoveries",
        "ec2:DescribeIpamResourceDiscoveryAssociations",
        "ec2:DescribeIpams",
        "ec2:DescribeIpamScopes",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteServerEndpoints",
        "ec2:DescribeRouteServerPeers",
        "ec2:DescribeRouteServers",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilterRules",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayMeteringPolicies",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
```

```
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVerifiedAccessEndpoints",
        "ec2:DescribeVerifiedAccessGroups",
        "ec2:DescribeVerifiedAccessInstanceLoggingConfigurations",
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessTrustProviders",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcBlockPublicAccessExclusions",
        "ec2:DescribeVpcEncryptionControls",
        "ec2:DescribeVpcEndpointAssociations",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConcentrators",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetAssociatedEnclaveCertificateIamRoles",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetIpamPrefixListResolverRules",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetRouteServerAssociations",
        "ec2:GetRouteServerPropagations",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayMeteringPolicyEntries",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:SearchTransitGatewayRoutes",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSubnetGroups",
```

```
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeServerlessCaches",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "es:GetApplication",
        "es:ListApplications",
        "es:ListTags",
        "frauddetector:BatchGetVariable",
        "frauddetector:DescribeDetector",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModelVersion",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListTagsForResource",
        "glue:DescribeIntegrations",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetCrawler",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetIntegrationResourceProperty",
        "glue:GetJob",
        "glue:GetRegistry",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetUsageProfile",
        "glue:ListCrawlers",
        "glue:ListIntegrationResourceProperties",
        "glue:ListJobs",
        "glue:ListRegistries",
        "glue:ListSchemas",
        "glue:ListSchemaVersions",
        "glue:ListTriggers",
```

```
        "glue:ListUsageProfiles",
        "identitystore:DescribeGroup",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "kms:DescribeCustomKeyStores",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:GetParametersForImport",
        "kms:GetPublicKey",
        "kms:ListAliases",
        "kms:ListGrants",
        "kms:ListKeyPolicies",
        "kms:ListKeyRotations",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "kms:ListRetirableGrants",
        "lambda:GetAlias",
        "lambda:GetCapacityProvider",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionScalingConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:ListAliases",
        "lambda:ListCapacityProviders",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListFunctions",
        "lambda:ListFunctionUrlConfigs",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "lightsail:GetAlarms",
```

```
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "memorydb:DescribeACLs",
        "memorydb:DescribeClusters",
        "memorydb:DescribeMultiRegionClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListTags",
        "neptune-graph:GetGraph",
        "neptune-graph:GetGraphSnapshot",
        "neptune-graph:GetPrivateGraphEndpoint",
        "neptune-graph:ListGraphs",
        "neptune-graph:ListGraphSnapshots",
        "neptune-graph:ListPrivateGraphEndpoints",
        "neptune-graph:ListTagsForResource",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListTagsForResource",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
```

```
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBProxyTargetGroups",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeIntegrations",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterDbRevisions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeIntegrations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeTags",
        "redshift:GetResourcePolicy",
        "route53globalresolver:GetAccessSource",
        "route53globalresolver:GetDNSView",
        "route53globalresolver:GetFirewallDomainList",
        "route53globalresolver:GetFirewallRule",
        "route53globalresolver:GetGlobalResolver",
        "route53globalresolver:GetHostedZoneAssociation",
        "route53globalresolver:ListAccessSources",
        "route53globalresolver:ListAccessTokens",
```

```
        "route53globalresolver:ListDNSViews",
        "route53globalresolver:ListFirewallDomainLists",
        "route53globalresolver:ListFirewallRules",
        "route53globalresolver:ListGlobalResolvers",
        "route53globalresolver:ListHostedZoneAssociations",
        "route53globalresolver:ListTagsForResource",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListRegionalBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointConfigurationForObjectLambda",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetMultiRegionAccessPoint",
```

```
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetObjectAcl",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsInstances",
        "s3:ListAccessGrantsLocations",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3:ListTagsForResource",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
        "s3express:GetAccessPointScope",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetInventoryConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:GetMetricsConfiguration",
        "s3express:ListAccessPointsForDirectoryBuckets",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:ListTagsForResource",
        "s3files:GetAccessPoint",
        "s3files:GetFileSystem",
        "s3files:GetFileSystemPolicy",
        "s3files:GetMountTarget",
        "s3files:GetSynchronizationConfiguration",
        "s3files:ListAccessPoints",
        "s3files:ListFileSystems",
        "s3files:ListMountTargets",
        "s3files:ListTagsForResource",
        "s3tables:GetNamespace",
        "s3tables:GetTable",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketMetricsConfiguration",
        "s3tables:GetTableBucketPolicy",
```

```
        "s3tables:GetTableBucketReplication",
        "s3tables:GetTableBucketStorageClass",
        "s3tables:GetTableMaintenanceConfiguration",
        "s3tables:GetTablePolicy",
        "s3tables:GetTableStorageClass",
        "s3tables:ListNamespaces",
        "s3tables:ListTableBuckets",
        "s3tables:ListTables",
        "s3tables:ListTagsForResource",
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:ListIndexes",
        "s3vectors:ListTagsForResource",
        "s3vectors:ListVectorBuckets",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "securityagent:BatchGetAgentSpaces",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetTargetDomains",
        "securityagent:GetApplication",
        "securityagent:ListAgentSpaces",
        "securityagent:ListApplications",
        "securityagent:ListIntegratedResources",
        "securityagent:ListPentests",
        "securityagent:ListTagsForResource",
        "securityagent:ListTargetDomains",
        "securityhub:BatchGetAutomationRules",
        "securityhub:BatchGetSecurityControls",
        "securityhub:DescribeHub",
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeSecurityHubV2",
        "securityhub:DescribeStandardsControls",
        "securityhub:GetAggregatorV2",
        "securityhub:GetAutomationRuleV2",
        "securityhub:GetConfigurationPolicy",
        "securityhub:GetConfigurationPolicyAssociation",
        "securityhub:GetConnectorV2",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindingAggregator",
        "securityhub:GetInsights",
        "securityhub:ListAggregatorsV2",
        "securityhub:ListAutomationRules",
```

```
        "securityhub:ListAutomationRulesV2",
        "securityhub:ListConfigurationPolicies",
        "securityhub:ListConfigurationPolicyAssociations",
        "securityhub:ListConnectorsV2",
        "securityhub:ListEnabledProductsForImport",
        "securityhub:ListFindingAggregators",
        "securityhub:ListOrganizationAdminAccounts",
        "securityhub:ListSecurityControlDefinitions",
        "securityhub:ListTagsForResource",
        "ssm:DescribeAssociation",
        "ssm:DescribeDocument",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeMaintenanceWindowTargets",
        "ssm:DescribeMaintenanceWindowTasks",
        "ssm:DescribeParameters",
        "ssm:DescribePatchBaselines",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetMaintenanceWindow",
        "ssm:GetMaintenanceWindowTask",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "sso-directory:DescribeGroup",
        "sso-directory:SearchGroups",
        "sts:GetCallerIdentity",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:ListTagsForResource",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeScheduledQuery",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListScheduledQueries",
        "timestream:ListTables",
        "timestream:ListTagsForResource"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

WellArchitectedConsoleFullAccess

Deskripsi: Menyediakan akses penuh ke AWS Well-Architected Alat melalui Konsol Manajemen AWS

`WellArchitectedConsoleFullAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `WellArchitectedConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2018, 18:19 UTC
- Waktu teredit: 09 Juli 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "wellarchitected:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "agent.wellarchitected.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "trustedadvisor:List*",
        "trustedadvisor:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:*:iam::*:role/aws-service-role/*/
AWSServiceRoleForWellArchitected*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "wellarchitected.amazonaws.com",
            "agent.wellarchitected.amazonaws.com",
            "metrics.wellarchitected.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:*:iam::*:role/aws-service-role/*/
AWSServiceRoleForWellArchitected*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreatePolicy",
        "iam:CreatePolicyVersion",
        "iam:DeletePolicyVersion"
      ],
```

```
      "Resource" : "arn:aws:iam::*:policy/service-role/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "wellarchitected.amazonaws.com",
            "agent.wellarchitected.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

WellArchitectedConsoleReadOnlyAccess

Deskripsi: Menyediakan akses read-only ke AWS Well-Architected Tool melalui Konsol Manajemen AWS

`WellArchitectedConsoleReadOnlyAccess`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `WellArchitectedConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2018, 18:21 UTC
- Waktu teredit: 09 Juli 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:Get*",
        "wellarchitected:List*",
        "wellarchitected:ExportLens",
        "organizations:DescribeAccount",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
```

```
        "trustedadvisor:List*",
        "trustedadvisor:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

WorkLinkServiceRolePolicy

Deskripsi: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Amazon WorkLink

`WorkLinkServiceRolePolicy`adalah kebijakan yang AWS dikelola.

Menggunakan kebijakan ini

Anda dapat melampirkan `WorkLinkServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Januari 2019, 19:03 UTC
- Waktu teredit: 23 Januari 2019, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, periksa AWS versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords"
      ],
      "Resource" : "arn:aws:kinesis:*:*:stream/AmazonWorkLink-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat kumpulan izin menggunakan kebijakan ter AWS kelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai dengan kebijakan ter AWS kelola dan beralih ke izin hak istimewa terendah

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.