



Guide de référence

AWS Stratégie gérée



AWS Stratégie gérée: Guide de référence

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

Les marques et la présentation commerciale d'Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n'est pas d'Amazon, d'une manière susceptible de créer une confusion parmi les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Que sont les politiques AWS gérées ?	1
Comprendre les pages de référence des politiques	1
Politiques gérées déconseillées AWS	2
AWS stratégies gérées	3
AccessAnalyzerServiceRolePolicy	57
Utilisation de cette politique	57
Détails de la politique	57
Version de la politique	57
Document de politique JSON	58
En savoir plus	60
AccountAccessManagerServiceRolePolicy	60
Utilisation de cette politique	61
Détails de la politique	61
Version de la politique	61
Document de politique JSON	61
En savoir plus	62
AccountManagementFromVercel	62
Utilisation de cette politique	62
Détails de la politique	62
Version de la politique	62
Document de politique JSON	63
En savoir plus	64
AdministratorAccess	64
Utilisation de cette politique	65
Détails de la politique	65
Version de la politique	65
Document de politique JSON	65
En savoir plus	65
AdministratorAccess-Amplify	66
Utilisation de cette politique	66
Détails de la politique	66
Version de la politique	66
Document de politique JSON	66
En savoir plus	77

AdministratorAccess-AWSElasticBeanstalk	77
Utilisation de cette politique	77
Détails de la politique	77
Version de la politique	77
Document de politique JSON	78
En savoir plus	86
AgentRegistryFullAccess	86
Utilisation de cette politique	86
Détails de la politique	86
Version de la politique	87
Document de politique JSON	87
En savoir plus	90
AgentRegistryReadOnlyAccess	91
Utilisation de cette politique	91
Détails de la politique	91
Version de la politique	91
Document de politique JSON	91
En savoir plus	92
AIDevOpsAgentAccessPolicy	92
Utilisation de cette politique	92
Détails de la politique	92
Version de la politique	92
Document de politique JSON	93
En savoir plus	115
AIDevOpsAgentActionsPolicy	116
Utilisation de cette politique	116
Détails de la politique	116
Version de la politique	116
Document de politique JSON	116
En savoir plus	117
AIDevOpsAgentFullAccess	117
Utilisation de cette politique	118
Détails de la politique	118
Version de la politique	118
Document de politique JSON	118
En savoir plus	120

AIDevOpsAgentReadOnlyAccess	121
Utilisation de cette politique	121
Détails de la politique	121
Version de la politique	121
Document de politique JSON	121
En savoir plus	122
AIDevOpsChannelAccessPolicy	122
Utilisation de cette politique	122
Détails de la politique	122
Version de la politique	122
Document de politique JSON	123
En savoir plus	123
AIDevOpsConstellationAccessPolicy	123
Utilisation de cette politique	124
Détails de la politique	124
Version de la politique	124
Document de politique JSON	124
En savoir plus	125
AIDevOpsOperatorAppAccessPolicy	125
Utilisation de cette politique	125
Détails de la politique	125
Version de la politique	125
Document de politique JSON	126
En savoir plus	129
AIDevOpsReleaseManagementVPCPolicy	129
Utilisation de cette politique	129
Détails de la politique	129
Version de la politique	129
Document de politique JSON	130
En savoir plus	132
AIOpsAssistantIncidentReportPolicy	133
Utilisation de cette politique	133
Détails de la politique	133
Version de la politique	133
Document de politique JSON	133
En savoir plus	134

AIOpsAssistantPolicy	134
Utilisation de cette politique	135
Détails de la politique	135
Version de la politique	135
Document de politique JSON	135
En savoir plus	156
AIOpsConsoleAdminPolicy	156
Utilisation de cette politique	156
Détails de la politique	156
Version de la politique	156
Document de politique JSON	157
En savoir plus	163
AIOpsOperatorAccess	163
Utilisation de cette politique	163
Détails de la politique	163
Version de la politique	163
Document de politique JSON	164
En savoir plus	166
AIOpsReadOnlyAccess	167
Utilisation de cette politique	167
Détails de la politique	167
Version de la politique	167
Document de politique JSON	167
En savoir plus	168
AlexaForBusinessDeviceSetup	168
Utilisation de cette politique	168
Détails de la politique	168
Version de la politique	169
Document de politique JSON	169
En savoir plus	169
AlexaForBusinessFullAccess	170
Utilisation de cette politique	170
Détails de la politique	170
Version de la politique	170
Document de politique JSON	170
En savoir plus	172

AlexaForBusinessGatewayExecution	172
Utilisation de cette politique	172
Détails de la politique	172
Version de la politique	172
Document de politique JSON	173
En savoir plus	173
AlexaForBusinessLifesizeDelegatedAccessPolicy	174
Utilisation de cette politique	174
Détails de la politique	174
Version de la politique	174
Document de politique JSON	174
En savoir plus	177
AlexaForBusinessNetworkProfileServicePolicy	177
Utilisation de cette politique	177
Détails de la politique	177
Version de la politique	177
Document de politique JSON	178
En savoir plus	178
AlexaForBusinessPolyDelegatedAccessPolicy	178
Utilisation de cette politique	179
Détails de la politique	179
Version de la politique	179
Document de politique JSON	179
En savoir plus	181
AlexaForBusinessReadOnlyAccess	181
Utilisation de cette politique	181
Détails de la politique	181
Version de la politique	181
Document de politique JSON	182
En savoir plus	182
AmazonAPIGatewayAdministrator	182
Utilisation de cette politique	182
Détails de la politique	183
Version de la politique	183
Document de politique JSON	183
En savoir plus	183

AmazonAPIGatewayInvokeFullAccess	184
Utilisation de cette politique	184
Détails de la politique	184
Version de la politique	184
Document de politique JSON	184
En savoir plus	185
AmazonAPIGatewayPushToCloudWatchLogs	185
Utilisation de cette politique	185
Détails de la politique	185
Version de la politique	185
Document de politique JSON	185
En savoir plus	186
AmazonAppFlowFullAccess	186
Utilisation de cette politique	186
Détails de la politique	186
Version de la politique	187
Document de politique JSON	187
En savoir plus	190
AmazonAppFlowReadOnlyAccess	190
Utilisation de cette politique	190
Détails de la politique	190
Version de la politique	190
Document de politique JSON	190
En savoir plus	191
AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy	191
Utilisation de cette politique	191
Détails de la politique	192
Version de la politique	192
Document de politique JSON	192
En savoir plus	193
AmazonAppStreamFullAccess	193
Utilisation de cette politique	194
Détails de la politique	194
Version de la politique	194
Document de politique JSON	194
En savoir plus	196

AmazonAppStreamPCAAccess	196
Utilisation de cette politique	196
Détails de la politique	196
Version de la politique	197
Document de politique JSON	197
En savoir plus	197
AmazonAppStreamReadOnlyAccess	197
Utilisation de cette politique	198
Détails de la politique	198
Version de la politique	198
Document de politique JSON	198
En savoir plus	198
AmazonAppStreamServiceAccess	199
Utilisation de cette politique	199
Détails de la politique	199
Version de la politique	199
Document de politique JSON	199
En savoir plus	200
AmazonAthenaFullAccess	201
Utilisation de cette politique	201
Détails de la politique	201
Version de la politique	201
Document de politique JSON	201
En savoir plus	205
AmazonAthenaServiceRolePolicy	205
Utilisation de cette politique	205
Détails de la politique	205
Version de la politique	206
Document de politique JSON	206
En savoir plus	206
AmazonAugmentedAIFullAccess	207
Utilisation de cette politique	207
Détails de la politique	207
Version de la politique	207
Document de politique JSON	207
En savoir plus	208

AmazonAugmentedAIHumanLoopFullAccess	208
Utilisation de cette politique	209
Détails de la politique	209
Version de la politique	209
Document de politique JSON	209
En savoir plus	209
AmazonAugmentedAIIntegratedAPIAccess	210
Utilisation de cette politique	210
Détails de la politique	210
Version de la politique	210
Document de politique JSON	210
En savoir plus	212
AmazonAuroraDSQLConsoleFullAccess	212
Utilisation de cette politique	212
Détails de la politique	212
Version de la politique	212
Document de politique JSON	213
En savoir plus	215
AmazonAuroraDSQLFullAccess	215
Utilisation de cette politique	215
Détails de la politique	215
Version de la politique	216
Document de politique JSON	216
En savoir plus	218
AmazonAuroraDSQLReadOnlyAccess	219
Utilisation de cette politique	219
Détails de la politique	219
Version de la politique	219
Document de politique JSON	219
En savoir plus	220
AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy	220
Utilisation de cette politique	220
Détails de la politique	221
Version de la politique	221
Document de politique JSON	221
En savoir plus	222

AmazonBedrockExternalWebSearchFullAccess	222
Utilisation de cette politique	222
Détails de la politique	222
Version de la politique	223
Document de politique JSON	223
En savoir plus	223
AmazonBedrockExternalWebSearchReadOnly	224
Utilisation de cette politique	224
Détails de la politique	224
Version de la politique	224
Document de politique JSON	224
En savoir plus	225
AmazonBedrockFullAccess	225
Utilisation de cette politique	225
Détails de la politique	225
Version de la politique	225
Document de politique JSON	226
En savoir plus	231
AmazonBedrockLimitedAccess	231
Utilisation de cette politique	231
Détails de la politique	231
Version de la politique	232
Document de politique JSON	232
En savoir plus	235
AmazonBedrockMantleFullAccess	235
Utilisation de cette politique	235
Détails de la politique	235
Version de la politique	235
Document de politique JSON	235
En savoir plus	236
AmazonBedrockMantleInferenceAccess	237
Utilisation de cette politique	237
Détails de la politique	237
Version de la politique	237
Document de politique JSON	237
En savoir plus	238

AmazonBedrockMantleReadOnly	239
Utilisation de cette politique	239
Détails de la politique	239
Version de la politique	239
Document de politique JSON	239
En savoir plus	240
AmazonBedrockMarketplaceAccess	240
Utilisation de cette politique	240
Détails de la politique	240
Version de la politique	240
Document de politique JSON	241
En savoir plus	245
AmazonBedrockReadOnly	245
Utilisation de cette politique	245
Détails de la politique	245
Version de la politique	246
Document de politique JSON	246
En savoir plus	247
AmazonBedrockStudioPermissionsBoundary	247
Utilisation de cette politique	248
Détails de la politique	248
Version de la politique	248
Document de politique JSON	248
En savoir plus	252
AmazonBedrockWebSearchFullAccess	252
Utilisation de cette politique	253
Détails de la politique	253
Version de la politique	253
Document de politique JSON	253
En savoir plus	253
AmazonBedrockWebSearchReadOnly	254
Utilisation de cette politique	254
Détails de la politique	254
Version de la politique	254
Document de politique JSON	254
En savoir plus	255

AmazonBioDiscoveryFullAccess	255
Utilisation de cette politique	255
Détails de la politique	255
Version de la politique	255
Document de politique JSON	256
En savoir plus	258
AmazonBioDiscoveryInAppFullAccess	258
Utilisation de cette politique	259
Détails de la politique	259
Version de la politique	259
Document de politique JSON	259
En savoir plus	261
AmazonBraketFullAccess	261
Utilisation de cette politique	261
Détails de la politique	261
Version de la politique	262
Document de politique JSON	262
En savoir plus	266
AmazonBraketJobsExecutionPolicy	267
Utilisation de cette politique	267
Détails de la politique	267
Version de la politique	267
Document de politique JSON	267
En savoir plus	270
AmazonBraketServiceRolePolicy	270
Utilisation de cette politique	270
Détails de la politique	271
Version de la politique	271
Document de politique JSON	271
En savoir plus	272
AmazonChimeFullAccess	272
Utilisation de cette politique	273
Détails de la politique	273
Version de la politique	273
Document de politique JSON	273
En savoir plus	275

AmazonChimeReadOnly	275
Utilisation de cette politique	276
Détails de la politique	276
Version de la politique	276
Document de politique JSON	276
En savoir plus	277
AmazonChimeSDK	277
Utilisation de cette politique	277
Détails de la politique	277
Version de la politique	277
Document de politique JSON	277
En savoir plus	278
AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy	279
Utilisation de cette politique	279
Détails de la politique	279
Version de la politique	279
Document de politique JSON	279
En savoir plus	281
AmazonChimeSDKMessagingServiceRolePolicy	281
Utilisation de cette politique	281
Détails de la politique	281
Version de la politique	281
Document de politique JSON	281
En savoir plus	282
AmazonChimeServiceRolePolicy	282
Utilisation de cette politique	283
Détails de la politique	283
Version de la politique	283
Document de politique JSON	283
En savoir plus	284
AmazonChimeTranscriptionServiceLinkedRolePolicy	284
Utilisation de cette politique	284
Détails de la politique	284
Version de la politique	284
Document de politique JSON	285
En savoir plus	285

AmazonChimeUserManagement	285
Utilisation de cette politique	285
Détails de la politique	285
Version de la politique	286
Document de politique JSON	286
En savoir plus	287
AmazonChimeVoiceConnectorServiceLinkedRolePolicy	287
Utilisation de cette politique	287
Détails de la politique	287
Version de la politique	288
Document de politique JSON	288
En savoir plus	290
AmazonCloudDirectoryFullAccess	290
Utilisation de cette politique	290
Détails de la politique	290
Version de la politique	290
Document de politique JSON	290
En savoir plus	291
AmazonCloudDirectoryReadOnlyAccess	291
Utilisation de cette politique	291
Détails de la politique	291
Version de la politique	292
Document de politique JSON	292
En savoir plus	292
AmazonCloudWatchEvidentlyFullAccess	293
Utilisation de cette politique	293
Détails de la politique	293
Version de la politique	293
Document de politique JSON	293
En savoir plus	296
AmazonCloudWatchEvidentlyReadOnlyAccess	296
Utilisation de cette politique	296
Détails de la politique	296
Version de la politique	296
Document de politique JSON	297
En savoir plus	297

AmazonCloudWatchEvidentlyServiceRolePolicy	297
Utilisation de cette politique	298
Détails de la politique	298
Version de la politique	298
Document de politique JSON	298
En savoir plus	300
AmazonCloudWatchRUMFullAccess	300
Utilisation de cette politique	300
Détails de la politique	300
Version de la politique	300
Document de politique JSON	300
En savoir plus	303
AmazonCloudWatchRUMReadOnlyAccess	303
Utilisation de cette politique	303
Détails de la politique	303
Version de la politique	303
Document de politique JSON	304
En savoir plus	305
AmazonCloudWatchRUMServiceRolePolicy	305
Utilisation de cette politique	305
Détails de la politique	305
Version de la politique	306
Document de politique JSON	306
En savoir plus	307
AmazonCodeCatalystFullAccess	307
Utilisation de cette politique	307
Détails de la politique	307
Version de la politique	307
Document de politique JSON	307
En savoir plus	308
AmazonCodeCatalystReadOnlyAccess	308
Utilisation de cette politique	309
Détails de la politique	309
Version de la politique	309
Document de politique JSON	309
En savoir plus	309

AmazonCodeCatalystSupportAccess	310
Utilisation de cette politique	310
Détails de la politique	310
Version de la politique	310
Document de politique JSON	310
En savoir plus	311
AmazonCodeGuruProfilerAgentAccess	311
Utilisation de cette politique	311
Détails de la politique	312
Version de la politique	312
Document de politique JSON	312
En savoir plus	312
AmazonCodeGuruProfilerFullAccess	313
Utilisation de cette politique	313
Détails de la politique	313
Version de la politique	313
Document de politique JSON	313
En savoir plus	314
AmazonCodeGuruProfilerReadOnlyAccess	314
Utilisation de cette politique	314
Détails de la politique	314
Version de la politique	315
Document de politique JSON	315
En savoir plus	315
AmazonCodeGuruReviewerFullAccess	316
Utilisation de cette politique	316
Détails de la politique	316
Version de la politique	316
Document de politique JSON	316
En savoir plus	319
AmazonCodeGuruReviewerReadOnlyAccess	319
Utilisation de cette politique	319
Détails de la politique	319
Version de la politique	319
Document de politique JSON	320
En savoir plus	320

AmazonCodeGuruReviewerServiceRolePolicy	320
Utilisation de cette politique	321
Détails de la politique	321
Version de la politique	321
Document de politique JSON	321
En savoir plus	323
AmazonCodeGuruSecurityFullAccess	323
Utilisation de cette politique	323
Détails de la politique	323
Version de la politique	324
Document de politique JSON	324
En savoir plus	324
AmazonCodeGuruSecurityScanAccess	324
Utilisation de cette politique	325
Détails de la politique	325
Version de la politique	325
Document de politique JSON	325
En savoir plus	326
AmazonCognitoDeveloperAuthenticatedIdentities	326
Utilisation de cette politique	326
Détails de la politique	326
Version de la politique	326
Document de politique JSON	327
En savoir plus	327
AmazonCognitoIdpEmailServiceRolePolicy	327
Utilisation de cette politique	327
Détails de la politique	328
Version de la politique	328
Document de politique JSON	328
En savoir plus	329
AmazonCognitoIdpServiceRolePolicy	329
Utilisation de cette politique	329
Détails de la politique	329
Version de la politique	329
Document de politique JSON	329
En savoir plus	330

AmazonCognitoPowerUser	330
Utilisation de cette politique	330
Détails de la politique	330
Version de la politique	330
Document de politique JSON	331
En savoir plus	332
AmazonCognitoReadOnly	332
Utilisation de cette politique	332
Détails de la politique	332
Version de la politique	333
Document de politique JSON	333
En savoir plus	334
AmazonCognitoUnAuthedIdentitiesSessionPolicy	334
Utilisation de cette politique	334
Détails de la politique	334
Version de la politique	334
Document de politique JSON	335
En savoir plus	336
AmazonCognitoUnauthenticatedIdentities	336
Utilisation de cette politique	336
Détails de la politique	336
Version de la politique	336
Document de politique JSON	337
En savoir plus	337
AmazonConnect_FullAccess	337
Utilisation de cette politique	337
Détails de la politique	337
Version de la politique	338
Document de politique JSON	338
En savoir plus	340
AmazonConnectCampaignsServiceLinkedRolePolicy	341
Utilisation de cette politique	341
Détails de la politique	341
Version de la politique	341
Document de politique JSON	341
En savoir plus	345

AmazonConnectReadOnlyAccess	345
Utilisation de cette politique	345
Détails de la politique	345
Version de la politique	345
Document de politique JSON	346
En savoir plus	346
AmazonConnectServiceLinkedRolePolicy	346
Utilisation de cette politique	347
Détails de la politique	347
Version de la politique	347
Document de politique JSON	347
En savoir plus	356
AmazonConnectSynchronizationServiceRolePolicy	356
Utilisation de cette politique	356
Détails de la politique	356
Version de la politique	356
Document de politique JSON	357
En savoir plus	359
AmazonConnectVoiceIDFullAccess	359
Utilisation de cette politique	359
Détails de la politique	359
Version de la politique	359
Document de politique JSON	359
En savoir plus	360
AmazonDataZoneBedrockModelConsumptionPolicy	360
Utilisation de cette politique	360
Détails de la politique	360
Version de la politique	360
Document de politique JSON	361
En savoir plus	363
AmazonDataZoneBedrockModelManagementPolicy	363
Utilisation de cette politique	363
Détails de la politique	364
Version de la politique	364
Document de politique JSON	364
En savoir plus	366

AmazonDataZoneDomainExecutionRolePolicy	366
Utilisation de cette politique	366
Détails de la politique	366
Version de la politique	367
Document de politique JSON	367
En savoir plus	370
AmazonDataZoneEnvironmentRolePermissionsBoundary	371
Utilisation de cette politique	371
Détails de la politique	371
Version de la politique	371
Document de politique JSON	371
En savoir plus	384
AmazonDataZoneFullAccess	384
Utilisation de cette politique	384
Détails de la politique	385
Version de la politique	385
Document de politique JSON	385
En savoir plus	394
AmazonDataZoneFullUserAccess	394
Utilisation de cette politique	394
Détails de la politique	394
Version de la politique	395
Document de politique JSON	395
En savoir plus	398
AmazonDataZoneGlueManageAccessRolePolicy	398
Utilisation de cette politique	399
Détails de la politique	399
Version de la politique	399
Document de politique JSON	399
En savoir plus	407
AmazonDataZonePortalFullAccessPolicy	407
Utilisation de cette politique	407
Détails de la politique	407
Version de la politique	408
Document de politique JSON	408
En savoir plus	408

AmazonDataZonePreviewConsoleFullAccess	408
Utilisation de cette politique	408
Détails de la politique	409
Version de la politique	409
Document de politique JSON	409
En savoir plus	411
AmazonDataZoneProjectDeploymentPermissionsBoundary	411
Utilisation de cette politique	411
Détails de la politique	411
Version de la politique	412
Document de politique JSON	412
En savoir plus	420
AmazonDataZoneProjectRolePermissionsBoundary	420
Utilisation de cette politique	420
Détails de la politique	420
Version de la politique	420
Document de politique JSON	421
En savoir plus	428
AmazonDataZoneRedshiftGlueProvisioningPolicy	428
Utilisation de cette politique	428
Détails de la politique	428
Version de la politique	429
Document de politique JSON	429
En savoir plus	436
AmazonDataZoneRedshiftManageAccessRolePolicy	437
Utilisation de cette politique	437
Détails de la politique	437
Version de la politique	437
Document de politique JSON	437
En savoir plus	441
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary	441
Utilisation de cette politique	441
Détails de la politique	441
Version de la politique	441
Document de politique JSON	442
En savoir plus	469

AmazonDataZoneSageMakerManageAccessRolePolicy	469
Utilisation de cette politique	469
Détails de la politique	469
Version de la politique	470
Document de politique JSON	470
En savoir plus	474
AmazonDataZoneSageMakerProvisioningRolePolicy	475
Utilisation de cette politique	475
Détails de la politique	475
Version de la politique	475
Document de politique JSON	475
En savoir plus	480
AmazonDetectiveFullAccess	480
Utilisation de cette politique	480
Détails de la politique	481
Version de la politique	481
Document de politique JSON	481
En savoir plus	482
AmazonDetectiveInvestigatorAccess	482
Utilisation de cette politique	482
Détails de la politique	482
Version de la politique	483
Document de politique JSON	483
En savoir plus	484
AmazonDetectiveMemberAccess	485
Utilisation de cette politique	485
Détails de la politique	485
Version de la politique	485
Document de politique JSON	485
En savoir plus	486
AmazonDetectiveOrganizationsAccess	486
Utilisation de cette politique	486
Détails de la politique	486
Version de la politique	487
Document de politique JSON	487
En savoir plus	488

AmazonDetectiveServiceLinkedRolePolicy	489
Utilisation de cette politique	489
Détails de la politique	489
Version de la politique	489
Document de politique JSON	489
En savoir plus	490
AmazonDevOpsGuruConsoleFullAccess	490
Utilisation de cette politique	490
Détails de la politique	490
Version de la politique	490
Document de politique JSON	491
En savoir plus	493
AmazonDevOpsGuruFullAccess	493
Utilisation de cette politique	493
Détails de la politique	493
Version de la politique	494
Document de politique JSON	494
En savoir plus	496
AmazonDevOpsGuruOrganizationsAccess	496
Utilisation de cette politique	496
Détails de la politique	497
Version de la politique	497
Document de politique JSON	497
En savoir plus	498
AmazonDevOpsGuruReadOnlyAccess	498
Utilisation de cette politique	499
Détails de la politique	499
Version de la politique	499
Document de politique JSON	499
En savoir plus	501
AmazonDevOpsGuruServiceRolePolicy	501
Utilisation de cette politique	501
Détails de la politique	501
Version de la politique	502
Document de politique JSON	502
En savoir plus	506

AmazonDMSCloudWatchLogsRole	506
Utilisation de cette politique	506
Détails de la politique	506
Version de la politique	506
Document de politique JSON	507
En savoir plus	508
AmazonDMSRedshiftS3Role	508
Utilisation de cette politique	509
Détails de la politique	509
Version de la politique	509
Document de politique JSON	509
En savoir plus	510
AmazonDMSVPCManagementRole	510
Utilisation de cette politique	510
Détails de la politique	510
Version de la politique	510
Document de politique JSON	511
En savoir plus	511
AmazonDocDB-ElasticServiceRolePolicy	511
Utilisation de cette politique	512
Détails de la politique	512
Version de la politique	512
Document de politique JSON	512
En savoir plus	513
AmazonDocDBConsoleFullAccess	513
Utilisation de cette politique	513
Détails de la politique	513
Version de la politique	513
Document de politique JSON	514
En savoir plus	518
AmazonDocDBElasticFullAccess	518
Utilisation de cette politique	518
Détails de la politique	519
Version de la politique	519
Document de politique JSON	519
En savoir plus	522

AmazonDocDBElasticReadOnlyAccess	522
Utilisation de cette politique	523
Détails de la politique	523
Version de la politique	523
Document de politique JSON	523
En savoir plus	524
AmazonDocDBFullAccess	524
Utilisation de cette politique	524
Détails de la politique	524
Version de la politique	524
Document de politique JSON	525
En savoir plus	527
AmazonDocDBReadOnlyAccess	528
Utilisation de cette politique	528
Détails de la politique	528
Version de la politique	528
Document de politique JSON	528
En savoir plus	530
AmazonDRSVPCManagement	530
Utilisation de cette politique	530
Détails de la politique	530
Version de la politique	531
Document de politique JSON	531
En savoir plus	532
AmazonDynamoDBFullAccess	532
Utilisation de cette politique	532
Détails de la politique	532
Version de la politique	532
Document de politique JSON	532
En savoir plus	535
AmazonDynamoDBFullAccess_v2	535
Utilisation de cette politique	535
Détails de la politique	535
Version de la politique	536
Document de politique JSON	536
En savoir plus	539

AmazonDynamoDBFullAccesswithDataPipeline	539
Utilisation de cette politique	540
Détails de la politique	540
Version de la politique	540
Document de politique JSON	540
En savoir plus	542
AmazonDynamoDBReadOnlyAccess	542
Utilisation de cette politique	542
Détails de la politique	543
Version de la politique	543
Document de politique JSON	543
En savoir plus	545
AmazonEBSCSIDriverEKSClusterScopedPolicy	545
Utilisation de cette politique	545
Détails de la politique	545
Version de la politique	546
Document de politique JSON	546
En savoir plus	551
AmazonEBSCSIDriverPolicy	551
Utilisation de cette politique	551
Détails de la politique	551
Version de la politique	551
Document de politique JSON	552
En savoir plus	556
AmazonEBSCSIDriverPolicyV2	556
Utilisation de cette politique	557
Détails de la politique	557
Version de la politique	557
Document de politique JSON	557
En savoir plus	562
AmazonEC2ContainerRegistryFullAccess	562
Utilisation de cette politique	562
Détails de la politique	562
Version de la politique	562
Document de politique JSON	563
En savoir plus	563

AmazonEC2ContainerRegistryPowerUser	564
Utilisation de cette politique	564
Détails de la politique	564
Version de la politique	564
Document de politique JSON	564
En savoir plus	565
AmazonEC2ContainerRegistryPullOnly	565
Utilisation de cette politique	565
Détails de la politique	565
Version de la politique	566
Document de politique JSON	566
En savoir plus	566
AmazonEC2ContainerRegistryReadOnly	567
Utilisation de cette politique	567
Détails de la politique	567
Version de la politique	567
Document de politique JSON	567
En savoir plus	568
AmazonEC2ContainerServiceAutoscaleRole	568
Utilisation de cette politique	568
Détails de la politique	568
Version de la politique	569
Document de politique JSON	569
En savoir plus	569
AmazonEC2ContainerServiceEventsRole	570
Utilisation de cette politique	570
Détails de la politique	570
Version de la politique	570
Document de politique JSON	570
En savoir plus	571
AmazonEC2ContainerServiceforEC2Role	571
Utilisation de cette politique	572
Détails de la politique	572
Version de la politique	572
Document de politique JSON	572
En savoir plus	573

AmazonEC2ContainerServiceRole	574
Utilisation de cette politique	574
Détails de la politique	574
Version de la politique	574
Document de politique JSON	574
En savoir plus	575
AmazonEC2FullAccess	575
Utilisation de cette politique	575
Détails de la politique	575
Version de la politique	575
Document de politique JSON	576
En savoir plus	577
AmazonEC2ImageReferencesAccessPolicy	577
Utilisation de cette politique	577
Détails de la politique	577
Version de la politique	577
Document de politique JSON	578
En savoir plus	578
AmazonEC2ReadOnlyAccess	579
Utilisation de cette politique	579
Détails de la politique	579
Version de la politique	579
Document de politique JSON	579
En savoir plus	580
AmazonEC2RoleforAWSCodeDeploy	580
Utilisation de cette politique	580
Détails de la politique	581
Version de la politique	581
Document de politique JSON	581
En savoir plus	581
AmazonEC2RoleforAWSCodeDeployLimited	582
Utilisation de cette politique	582
Détails de la politique	582
Version de la politique	582
Document de politique JSON	582
En savoir plus	583

AmazonEC2RoleforDataPipelineRole	583
Utilisation de cette politique	583
Détails de la politique	584
Version de la politique	584
Document de politique JSON	584
En savoir plus	585
AmazonEC2RoleforSSM	585
Utilisation de cette politique	585
Détails de la politique	585
Version de la politique	585
Document de politique JSON	586
En savoir plus	588
AmazonEC2RolePolicyForLaunchWizard	588
Utilisation de cette politique	588
Détails de la politique	588
Version de la politique	589
Document de politique JSON	589
En savoir plus	593
AmazonEC2SpotFleetAutoscaleRole	594
Utilisation de cette politique	594
Détails de la politique	594
Version de la politique	594
Document de politique JSON	594
En savoir plus	595
AmazonEC2SpotFleetTaggingRole	595
Utilisation de cette politique	596
Détails de la politique	596
Version de la politique	596
Document de politique JSON	596
En savoir plus	597
AmazonECS_FullAccess	598
Utilisation de cette politique	598
Détails de la politique	598
Version de la politique	598
Document de politique JSON	598
En savoir plus	604

AmazonECSComputeServiceRolePolicy	605
Utilisation de cette politique	605
Détails de la politique	605
Version de la politique	605
Document de politique JSON	605
En savoir plus	607
AmazonECSInfrastructureRoleforExpressGatewayServices	607
Utilisation de cette politique	607
Détails de la politique	607
Version de la politique	607
Document de politique JSON	608
En savoir plus	614
AmazonECSInfrastructureRoleForGatewayHostSharedALB	614
Utilisation de cette politique	614
Détails de la politique	614
Version de la politique	615
Document de politique JSON	615
En savoir plus	620
AmazonECSInfrastructureRolePolicyForLoadBalancers	620
Utilisation de cette politique	621
Détails de la politique	621
Version de la politique	621
Document de politique JSON	621
En savoir plus	622
AmazonECSInfrastructureRolePolicyForManagedInstances	623
Utilisation de cette politique	623
Détails de la politique	623
Version de la politique	623
Document de politique JSON	623
En savoir plus	628
AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity	628
Utilisation de cette politique	628
Détails de la politique	629
Version de la politique	629
Document de politique JSON	629
En savoir plus	631

AmazonECSInfrastructureRolePolicyForVolumes	632
Utilisation de cette politique	632
Détails de la politique	632
Version de la politique	632
Document de politique JSON	632
En savoir plus	635
AmazonECSInfrastructureRolePolicyForVpcLattice	635
Utilisation de cette politique	635
Détails de la politique	635
Version de la politique	635
Document de politique JSON	636
En savoir plus	637
AmazonECSInstanceRolePolicyForManagedInstances	637
Utilisation de cette politique	638
Détails de la politique	638
Version de la politique	638
Document de politique JSON	638
En savoir plus	639
AmazonECSServiceRolePolicy	640
Utilisation de cette politique	640
Détails de la politique	640
Version de la politique	640
Document de politique JSON	640
En savoir plus	646
AmazonECSTaskExecutionRolePolicy	646
Utilisation de cette politique	646
Détails de la politique	646
Version de la politique	646
Document de politique JSON	647
En savoir plus	647
AmazonEFSCSIDriverPolicy	647
Utilisation de cette politique	647
Détails de la politique	648
Version de la politique	648
Document de politique JSON	648
En savoir plus	649

AmazonEKS_CNI_Policy	650
Utilisation de cette politique	650
Détails de la politique	650
Version de la politique	650
Document de politique JSON	650
En savoir plus	651
AmazonEKSBLOCKStoragePolicy	652
Utilisation de cette politique	652
Détails de la politique	652
Version de la politique	652
Document de politique JSON	652
En savoir plus	654
AmazonEKSBLOCKStoragePolicyV2	655
Utilisation de cette politique	655
Détails de la politique	655
Version de la politique	655
Document de politique JSON	655
En savoir plus	658
AmazonEKSClusterPolicy	658
Utilisation de cette politique	658
Détails de la politique	658
Version de la politique	659
Document de politique JSON	659
En savoir plus	661
AmazonEKSComputePolicy	661
Utilisation de cette politique	661
Détails de la politique	661
Version de la politique	662
Document de politique JSON	662
En savoir plus	665
AmazonEKSCONNECTORServiceRolePolicy	665
Utilisation de cette politique	665
Détails de la politique	665
Version de la politique	665
Document de politique JSON	666
En savoir plus	668

AmazonEKSDashboardConsoleReadOnly	668
Utilisation de cette politique	668
Détails de la politique	668
Version de la politique	668
Document de politique JSON	668
En savoir plus	669
AmazonEKSDashboardServiceRolePolicy	670
Utilisation de cette politique	670
Détails de la politique	670
Version de la politique	670
Document de politique JSON	670
En savoir plus	671
AmazonEKSFargatePodExecutionRolePolicy	671
Utilisation de cette politique	671
Détails de la politique	671
Version de la politique	672
Document de politique JSON	672
En savoir plus	672
AmazonEKSFargateServiceRolePolicy	673
Utilisation de cette politique	673
Détails de la politique	673
Version de la politique	673
Document de politique JSON	673
En savoir plus	674
AmazonEKSLoadBalancingPolicy	674
Utilisation de cette politique	674
Détails de la politique	674
Version de la politique	674
Document de politique JSON	675
En savoir plus	680
AmazonEKSLocalOutpostClusterPolicy	681
Utilisation de cette politique	681
Détails de la politique	681
Version de la politique	681
Document de politique JSON	681
En savoir plus	683

AmazonEKSLocalOutpostServiceRolePolicy	683
Utilisation de cette politique	683
Détails de la politique	684
Version de la politique	684
Document de politique JSON	684
En savoir plus	690
AmazonEKSMCPReadOnlyAccess	690
Utilisation de cette politique	690
Détails de la politique	690
Version de la politique	690
Document de politique JSON	691
En savoir plus	692
AmazonEKSNetworkingPolicy	693
Utilisation de cette politique	693
Détails de la politique	693
Version de la politique	693
Document de politique JSON	693
En savoir plus	695
AmazonEKSServicePolicy	696
Utilisation de cette politique	696
Détails de la politique	696
Version de la politique	696
Document de politique JSON	696
En savoir plus	698
AmazonEKSServiceRolePolicy	698
Utilisation de cette politique	699
Détails de la politique	699
Version de la politique	699
Document de politique JSON	699
En savoir plus	707
AmazonEKSVPCResourceController	708
Utilisation de cette politique	708
Détails de la politique	708
Version de la politique	708
Document de politique JSON	708
En savoir plus	709

AmazonEKSWorkerNodeMinimalPolicy	709
Utilisation de cette politique	709
Détails de la politique	709
Version de la politique	710
Document de politique JSON	710
En savoir plus	710
AmazonEKSWorkerNodePolicy	710
Utilisation de cette politique	711
Détails de la politique	711
Version de la politique	711
Document de politique JSON	711
En savoir plus	712
AmazonElastiCacheFullAccess	712
Utilisation de cette politique	712
Détails de la politique	712
Version de la politique	712
Document de politique JSON	713
En savoir plus	716
AmazonElastiCacheReadOnlyAccess	716
Utilisation de cette politique	716
Détails de la politique	716
Version de la politique	716
Document de politique JSON	717
En savoir plus	717
AmazonElasticContainerRegistryPublicFullAccess	717
Utilisation de cette politique	717
Détails de la politique	718
Version de la politique	718
Document de politique JSON	718
En savoir plus	718
AmazonElasticContainerRegistryPublicPowerUser	719
Utilisation de cette politique	719
Détails de la politique	719
Version de la politique	719
Document de politique JSON	719
En savoir plus	720

AmazonElasticContainerRegistryPublicReadOnly	720
Utilisation de cette politique	720
Détails de la politique	720
Version de la politique	721
Document de politique JSON	721
En savoir plus	721
AmazonElasticFileSystemClientFullAccess	722
Utilisation de cette politique	722
Détails de la politique	722
Version de la politique	722
Document de politique JSON	722
En savoir plus	723
AmazonElasticFileSystemClientReadOnlyAccess	723
Utilisation de cette politique	723
Détails de la politique	723
Version de la politique	723
Document de politique JSON	724
En savoir plus	724
AmazonElasticFileSystemClientReadWriteAccess	724
Utilisation de cette politique	724
Détails de la politique	725
Version de la politique	725
Document de politique JSON	725
En savoir plus	725
AmazonElasticFileSystemFullAccess	726
Utilisation de cette politique	726
Détails de la politique	726
Version de la politique	726
Document de politique JSON	726
En savoir plus	728
AmazonElasticFileSystemReadOnlyAccess	728
Utilisation de cette politique	729
Détails de la politique	729
Version de la politique	729
Document de politique JSON	729
En savoir plus	730

AmazonElasticFileSystemServiceRolePolicy	730
Utilisation de cette politique	730
Détails de la politique	730
Version de la politique	731
Document de politique JSON	731
En savoir plus	733
AmazonElasticFileSystemsUtils	733
Utilisation de cette politique	733
Détails de la politique	733
Version de la politique	734
Document de politique JSON	734
En savoir plus	736
AmazonElasticMapReduceEditorsRole	736
Utilisation de cette politique	736
Détails de la politique	736
Version de la politique	737
Document de politique JSON	737
En savoir plus	738
AmazonElasticMapReduceforAutoScalingRole	738
Utilisation de cette politique	738
Détails de la politique	738
Version de la politique	739
Document de politique JSON	739
En savoir plus	739
AmazonElasticMapReduceforEC2Role	739
Utilisation de cette politique	740
Détails de la politique	740
Version de la politique	740
Document de politique JSON	740
En savoir plus	742
AmazonElasticMapReduceFullAccess	742
Utilisation de cette politique	742
Détails de la politique	742
Version de la politique	742
Document de politique JSON	743
En savoir plus	744

AmazonElasticMapReducePlacementGroupPolicy	745
Utilisation de cette politique	745
Détails de la politique	745
Version de la politique	745
Document de politique JSON	745
En savoir plus	746
AmazonElasticMapReduceReadOnlyAccess	746
Utilisation de cette politique	746
Détails de la politique	746
Version de la politique	747
Document de politique JSON	747
En savoir plus	747
AmazonElasticMapReduceRole	748
Utilisation de cette politique	748
Détails de la politique	748
Version de la politique	748
Document de politique JSON	748
En savoir plus	750
AmazonElasticsearchServiceRolePolicy	751
Utilisation de cette politique	751
Détails de la politique	751
Version de la politique	751
Document de politique JSON	751
En savoir plus	754
AmazonElasticTranscoder_FullAccess	755
Utilisation de cette politique	755
Détails de la politique	755
Version de la politique	755
Document de politique JSON	755
En savoir plus	756
AmazonElasticTranscoder_JobsSubmitter	756
Utilisation de cette politique	756
Détails de la politique	757
Version de la politique	757
Document de politique JSON	757
En savoir plus	757

AmazonElasticTranscoder_ReadOnlyAccess	758
Utilisation de cette politique	758
Détails de la politique	758
Version de la politique	758
Document de politique JSON	758
En savoir plus	759
AmazonElasticTranscoderRole	759
Utilisation de cette politique	759
Détails de la politique	759
Version de la politique	760
Document de politique JSON	760
En savoir plus	761
AmazonEMRCleanupPolicy	761
Utilisation de cette politique	761
Détails de la politique	761
Version de la politique	761
Document de politique JSON	761
En savoir plus	762
AmazonEMRContainersServiceRolePolicy	762
Utilisation de cette politique	763
Détails de la politique	763
Version de la politique	763
Document de politique JSON	763
En savoir plus	766
AmazonEMRFullAccessPolicy_v2	766
Utilisation de cette politique	766
Détails de la politique	766
Version de la politique	766
Document de politique JSON	766
En savoir plus	770
AmazonEMRReadOnlyAccessPolicy_v2	770
Utilisation de cette politique	770
Détails de la politique	770
Version de la politique	771
Document de politique JSON	771
En savoir plus	772

AmazonEMRServerlessServiceRolePolicy	772
Utilisation de cette politique	772
Détails de la politique	772
Version de la politique	772
Document de politique JSON	773
En savoir plus	774
AmazonEMRServicePolicy_v2	774
Utilisation de cette politique	774
Détails de la politique	774
Version de la politique	774
Document de politique JSON	774
En savoir plus	783
AmazonEMRServicePolicyForSessions	783
Utilisation de cette politique	784
Détails de la politique	784
Version de la politique	784
Document de politique JSON	784
En savoir plus	788
AmazonESCognitoAccess	788
Utilisation de cette politique	788
Détails de la politique	788
Version de la politique	788
Document de politique JSON	789
En savoir plus	789
AmazonESFullAccess	790
Utilisation de cette politique	790
Détails de la politique	790
Version de la politique	790
Document de politique JSON	790
En savoir plus	791
AmazonESReadOnlyAccess	791
Utilisation de cette politique	791
Détails de la politique	791
Version de la politique	791
Document de politique JSON	792
En savoir plus	792

AmazonEventBridgeApiDestinationsServiceRolePolicy	792
Utilisation de cette politique	792
Détails de la politique	792
Version de la politique	793
Document de politique JSON	793
En savoir plus	794
AmazonEventBridgeFullAccess	794
Utilisation de cette politique	794
Détails de la politique	794
Version de la politique	795
Document de politique JSON	795
En savoir plus	797
AmazonEventBridgePipesFullAccess	797
Utilisation de cette politique	797
Détails de la politique	797
Version de la politique	797
Document de politique JSON	798
En savoir plus	798
AmazonEventBridgePipesOperatorAccess	799
Utilisation de cette politique	799
Détails de la politique	799
Version de la politique	799
Document de politique JSON	799
En savoir plus	800
AmazonEventBridgePipesReadOnlyAccess	800
Utilisation de cette politique	800
Détails de la politique	800
Version de la politique	800
Document de politique JSON	801
En savoir plus	801
AmazonEventBridgeReadOnlyAccess	801
Utilisation de cette politique	801
Détails de la politique	801
Version de la politique	802
Document de politique JSON	802
En savoir plus	803

AmazonEventBridgeSchedulerFullAccess	803
Utilisation de cette politique	804
Détails de la politique	804
Version de la politique	804
Document de politique JSON	804
En savoir plus	805
AmazonEventBridgeSchedulerReadOnlyAccess	805
Utilisation de cette politique	805
Détails de la politique	805
Version de la politique	805
Document de politique JSON	806
En savoir plus	806
AmazonEventBridgeSchemasFullAccess	806
Utilisation de cette politique	806
Détails de la politique	807
Version de la politique	807
Document de politique JSON	807
En savoir plus	808
AmazonEventBridgeSchemasReadOnlyAccess	808
Utilisation de cette politique	808
Détails de la politique	808
Version de la politique	809
Document de politique JSON	809
En savoir plus	809
AmazonEventBridgeSchemasServiceRolePolicy	810
Utilisation de cette politique	810
Détails de la politique	810
Version de la politique	810
Document de politique JSON	810
En savoir plus	811
AmazonEVSServiceRolePolicy	811
Utilisation de cette politique	811
Détails de la politique	811
Version de la politique	812
Document de politique JSON	812
En savoir plus	817

AmazonFISServiceRolePolicy	817
Utilisation de cette politique	817
Détails de la politique	817
Version de la politique	818
Document de politique JSON	818
En savoir plus	819
AmazonForecastFullAccess	820
Utilisation de cette politique	820
Détails de la politique	820
Version de la politique	820
Document de politique JSON	820
En savoir plus	821
AmazonFraudDetectorFullAccessPolicy	821
Utilisation de cette politique	821
Détails de la politique	821
Version de la politique	822
Document de politique JSON	822
En savoir plus	823
AmazonFreeRTOSFullAccess	823
Utilisation de cette politique	823
Détails de la politique	823
Version de la politique	824
Document de politique JSON	824
En savoir plus	824
AmazonFreeRTOSOTAUpdate	824
Utilisation de cette politique	824
Détails de la politique	825
Version de la politique	825
Document de politique JSON	825
En savoir plus	826
AmazonFSxConsoleFullAccess	827
Utilisation de cette politique	827
Détails de la politique	827
Version de la politique	827
Document de politique JSON	827
En savoir plus	831

AmazonFSxConsoleReadOnlyAccess	831
Utilisation de cette politique	831
Détails de la politique	831
Version de la politique	831
Document de politique JSON	832
En savoir plus	832
AmazonFSxFullAccess	832
Utilisation de cette politique	833
Détails de la politique	833
Version de la politique	833
Document de politique JSON	833
En savoir plus	837
AmazonFSxReadOnlyAccess	837
Utilisation de cette politique	838
Détails de la politique	838
Version de la politique	838
Document de politique JSON	838
En savoir plus	838
AmazonFSxServiceRolePolicy	839
Utilisation de cette politique	839
Détails de la politique	839
Version de la politique	839
Document de politique JSON	839
En savoir plus	842
AmazonGlacierFullAccess	842
Utilisation de cette politique	842
Détails de la politique	842
Version de la politique	843
Document de politique JSON	843
En savoir plus	843
AmazonGlacierReadOnlyAccess	843
Utilisation de cette politique	844
Détails de la politique	844
Version de la politique	844
Document de politique JSON	844
En savoir plus	845

AmazonGrafanaAthenaAccess	845
Utilisation de cette politique	845
Détails de la politique	845
Version de la politique	845
Document de politique JSON	846
En savoir plus	847
AmazonGrafanaCloudWatchAccess	848
Utilisation de cette politique	848
Détails de la politique	848
Version de la politique	848
Document de politique JSON	848
En savoir plus	850
AmazonGrafanaRedshiftAccess	850
Utilisation de cette politique	850
Détails de la politique	850
Version de la politique	850
Document de politique JSON	850
En savoir plus	852
AmazonGrafanaServiceLinkedRolePolicy	852
Utilisation de cette politique	852
Détails de la politique	852
Version de la politique	852
Document de politique JSON	853
En savoir plus	854
AmazonGuardDutyFullAccess	854
Utilisation de cette politique	854
Détails de la politique	854
Version de la politique	855
Document de politique JSON	855
En savoir plus	856
AmazonGuardDutyFullAccess_v2	856
Utilisation de cette politique	857
Détails de la politique	857
Version de la politique	857
Document de politique JSON	857
En savoir plus	859

AmazonGuardDutyMalwareProtectionServiceRolePolicy	859
Utilisation de cette politique	860
Détails de la politique	860
Version de la politique	860
Document de politique JSON	860
En savoir plus	865
AmazonGuardDutyReadOnlyAccess	865
Utilisation de cette politique	865
Détails de la politique	865
Version de la politique	865
Document de politique JSON	865
En savoir plus	866
AmazonGuardDutyServiceRolePolicy	866
Utilisation de cette politique	866
Détails de la politique	867
Version de la politique	867
Document de politique JSON	867
En savoir plus	874
AmazonHealthLakeFullAccess	874
Utilisation de cette politique	874
Détails de la politique	874
Version de la politique	874
Document de politique JSON	875
En savoir plus	875
AmazonHealthLakeReadOnlyAccess	875
Utilisation de cette politique	876
Détails de la politique	876
Version de la politique	876
Document de politique JSON	876
En savoir plus	877
AmazonHoneycodeFullAccess	877
Utilisation de cette politique	877
Détails de la politique	877
Version de la politique	877
Document de politique JSON	878
En savoir plus	878

AmazonHoneycodeReadOnlyAccess	878
Utilisation de cette politique	878
Détails de la politique	879
Version de la politique	879
Document de politique JSON	879
En savoir plus	879
AmazonHoneycodeServiceRolePolicy	880
Utilisation de cette politique	880
Détails de la politique	880
Version de la politique	880
Document de politique JSON	880
En savoir plus	881
AmazonHoneycodeTeamAssociationFullAccess	881
Utilisation de cette politique	881
Détails de la politique	881
Version de la politique	881
Document de politique JSON	882
En savoir plus	882
AmazonHoneycodeTeamAssociationReadOnlyAccess	882
Utilisation de cette politique	882
Détails de la politique	882
Version de la politique	883
Document de politique JSON	883
En savoir plus	883
AmazonHoneycodeWorkbookFullAccess	883
Utilisation de cette politique	884
Détails de la politique	884
Version de la politique	884
Document de politique JSON	884
En savoir plus	885
AmazonHoneycodeWorkbookReadOnlyAccess	885
Utilisation de cette politique	885
Détails de la politique	885
Version de la politique	885
Document de politique JSON	886
En savoir plus	886

AmazonInspector2AgentlessServiceRolePolicy	886
Utilisation de cette politique	887
Détails de la politique	887
Version de la politique	887
Document de politique JSON	887
En savoir plus	892
AmazonInspector2AmiScanServiceRolePolicy	892
Utilisation de cette politique	892
Détails de la politique	892
Version de la politique	892
Document de politique JSON	893
En savoir plus	896
AmazonInspector2FullAccess	896
Utilisation de cette politique	896
Détails de la politique	897
Version de la politique	897
Document de politique JSON	897
En savoir plus	898
AmazonInspector2FullAccess_v2	898
Utilisation de cette politique	899
Détails de la politique	899
Version de la politique	899
Document de politique JSON	899
En savoir plus	902
AmazonInspector2ManagedCisPolicy	903
Utilisation de cette politique	903
Détails de la politique	903
Version de la politique	903
Document de politique JSON	903
En savoir plus	904
AmazonInspector2ManagedTelemetryPolicy	904
Utilisation de cette politique	904
Détails de la politique	904
Version de la politique	904
Document de politique JSON	905
En savoir plus	905

AmazonInspector2ReadOnlyAccess	905
Utilisation de cette politique	906
Détails de la politique	906
Version de la politique	906
Document de politique JSON	906
En savoir plus	908
AmazonInspector2ServiceRolePolicy	908
Utilisation de cette politique	908
Détails de la politique	908
Version de la politique	908
Document de politique JSON	909
En savoir plus	917
AmazonInspector2ThirdPartyServiceRolePolicy	917
Utilisation de cette politique	917
Détails de la politique	917
Version de la politique	917
Document de politique JSON	918
En savoir plus	922
AmazonInspectorFullAccess	922
Utilisation de cette politique	922
Détails de la politique	923
Version de la politique	923
Document de politique JSON	923
En savoir plus	924
AmazonInspectorReadOnlyAccess	924
Utilisation de cette politique	924
Détails de la politique	924
Version de la politique	925
Document de politique JSON	925
En savoir plus	925
AmazonInspectorServiceRolePolicy	926
Utilisation de cette politique	926
Détails de la politique	926
Version de la politique	926
Document de politique JSON	926
En savoir plus	928

AmazonKendraFullAccess	928
Utilisation de cette politique	928
Détails de la politique	928
Version de la politique	928
Document de politique JSON	928
En savoir plus	930
AmazonKendraReadOnlyAccess	930
Utilisation de cette politique	931
Détails de la politique	931
Version de la politique	931
Document de politique JSON	931
En savoir plus	932
AmazonKeyspacesFullAccess	932
Utilisation de cette politique	932
Détails de la politique	932
Version de la politique	932
Document de politique JSON	932
En savoir plus	935
AmazonKeyspacesReadOnlyAccess	935
Utilisation de cette politique	935
Détails de la politique	935
Version de la politique	935
Document de politique JSON	935
En savoir plus	936
AmazonKeyspacesReadOnlyAccess_v2	936
Utilisation de cette politique	937
Détails de la politique	937
Version de la politique	937
Document de politique JSON	937
En savoir plus	938
AmazonKinesisAnalyticsFullAccess	938
Utilisation de cette politique	938
Détails de la politique	938
Version de la politique	939
Document de politique JSON	939
En savoir plus	940

AmazonKinesisAnalyticsReadOnly	941
Utilisation de cette politique	941
Détails de la politique	941
Version de la politique	941
Document de politique JSON	941
En savoir plus	942
AmazonKinesisFirehoseFullAccess	943
Utilisation de cette politique	943
Détails de la politique	943
Version de la politique	943
Document de politique JSON	943
En savoir plus	944
AmazonKinesisFirehoseReadOnlyAccess	944
Utilisation de cette politique	944
Détails de la politique	944
Version de la politique	944
Document de politique JSON	945
En savoir plus	945
AmazonKinesisFullAccess	945
Utilisation de cette politique	945
Détails de la politique	945
Version de la politique	946
Document de politique JSON	946
En savoir plus	946
AmazonKinesisReadOnlyAccess	946
Utilisation de cette politique	946
Détails de la politique	947
Version de la politique	947
Document de politique JSON	947
En savoir plus	947
AmazonKinesisVideoStreamsFullAccess	948
Utilisation de cette politique	948
Détails de la politique	948
Version de la politique	948
Document de politique JSON	948
En savoir plus	949

AmazonKinesisVideoStreamsReadOnlyAccess	949
Utilisation de cette politique	949
Détails de la politique	949
Version de la politique	949
Document de politique JSON	949
En savoir plus	950
AmazonLaunchWizard_Fullaccess	950
Utilisation de cette politique	950
Détails de la politique	950
Version de la politique	951
Document de politique JSON	951
En savoir plus	965
AmazonLaunchWizardFullAccessV2	965
Utilisation de cette politique	965
Détails de la politique	965
Version de la politique	966
Document de politique JSON	966
En savoir plus	987
AmazonLexChannelsAccess	987
Utilisation de cette politique	988
Détails de la politique	988
Version de la politique	988
Document de politique JSON	988
En savoir plus	989
AmazonLexFullAccess	989
Utilisation de cette politique	989
Détails de la politique	989
Version de la politique	989
Document de politique JSON	989
En savoir plus	995
AmazonLexReadOnly	995
Utilisation de cette politique	995
Détails de la politique	995
Version de la politique	995
Document de politique JSON	996
En savoir plus	997

AmazonLexReplicationPolicy	997
Utilisation de cette politique	998
Détails de la politique	998
Version de la politique	998
Document de politique JSON	998
En savoir plus	1000
AmazonLexRunBotsOnly	1001
Utilisation de cette politique	1001
Détails de la politique	1001
Version de la politique	1001
Document de politique JSON	1001
En savoir plus	1002
AmazonLexV2BotPolicy	1002
Utilisation de cette politique	1002
Détails de la politique	1002
Version de la politique	1002
Document de politique JSON	1003
En savoir plus	1003
AmazonLookoutEquipmentFullAccess	1003
Utilisation de cette politique	1003
Détails de la politique	1003
Version de la politique	1004
Document de politique JSON	1004
En savoir plus	1005
AmazonLookoutEquipmentReadOnlyAccess	1005
Utilisation de cette politique	1005
Détails de la politique	1006
Version de la politique	1006
Document de politique JSON	1006
En savoir plus	1006
AmazonLookoutMetricsFullAccess	1007
Utilisation de cette politique	1007
Détails de la politique	1007
Version de la politique	1007
Document de politique JSON	1007
En savoir plus	1008

AmazonLookoutMetricsReadOnlyAccess	1008
Utilisation de cette politique	1008
Détails de la politique	1008
Version de la politique	1009
Document de politique JSON	1009
En savoir plus	1009
AmazonLookoutVisionConsoleFullAccess	1010
Utilisation de cette politique	1010
Détails de la politique	1010
Version de la politique	1010
Document de politique JSON	1010
En savoir plus	1013
AmazonLookoutVisionConsoleReadOnlyAccess	1013
Utilisation de cette politique	1013
Détails de la politique	1013
Version de la politique	1013
Document de politique JSON	1013
En savoir plus	1015
AmazonLookoutVisionFullAccess	1015
Utilisation de cette politique	1015
Détails de la politique	1015
Version de la politique	1015
Document de politique JSON	1016
En savoir plus	1016
AmazonLookoutVisionReadOnlyAccess	1016
Utilisation de cette politique	1016
Détails de la politique	1016
Version de la politique	1017
Document de politique JSON	1017
En savoir plus	1017
AmazonMachineLearningBatchPredictionsAccess	1018
Utilisation de cette politique	1018
Détails de la politique	1018
Version de la politique	1018
Document de politique JSON	1018
En savoir plus	1019

AmazonMachineLearningCreateOnlyAccess	1019
Utilisation de cette politique	1019
Détails de la politique	1019
Version de la politique	1019
Document de politique JSON	1020
En savoir plus	1020
AmazonMachineLearningFullAccess	1020
Utilisation de cette politique	1020
Détails de la politique	1021
Version de la politique	1021
Document de politique JSON	1021
En savoir plus	1021
AmazonMachineLearningManageRealTimeEndpointOnlyAccess	1022
Utilisation de cette politique	1022
Détails de la politique	1022
Version de la politique	1022
Document de politique JSON	1022
En savoir plus	1023
AmazonMachineLearningReadOnlyAccess	1023
Utilisation de cette politique	1023
Détails de la politique	1023
Version de la politique	1023
Document de politique JSON	1024
En savoir plus	1024
AmazonMachineLearningRealTimePredictionOnlyAccess	1024
Utilisation de cette politique	1024
Détails de la politique	1024
Version de la politique	1025
Document de politique JSON	1025
En savoir plus	1025
AmazonMachineLearningRoleforRedshiftDataSourceV3	1025
Utilisation de cette politique	1026
Détails de la politique	1026
Version de la politique	1026
Document de politique JSON	1026
En savoir plus	1027

AmazonMacieFullAccess	1027
Utilisation de cette politique	1027
Détails de la politique	1027
Version de la politique	1028
Document de politique JSON	1028
En savoir plus	1029
AmazonMacieHandshakeRole	1029
Utilisation de cette politique	1029
Détails de la politique	1029
Version de la politique	1029
Document de politique JSON	1029
En savoir plus	1030
AmazonMacieReadOnlyAccess	1030
Utilisation de cette politique	1030
Détails de la politique	1030
Version de la politique	1031
Document de politique JSON	1031
En savoir plus	1031
AmazonMacieServiceRole	1031
Utilisation de cette politique	1032
Détails de la politique	1032
Version de la politique	1032
Document de politique JSON	1032
En savoir plus	1032
AmazonMacieServiceRolePolicy	1033
Utilisation de cette politique	1033
Détails de la politique	1033
Version de la politique	1033
Document de politique JSON	1033
En savoir plus	1035
AmazonManagedBlockchainConsoleFullAccess	1035
Utilisation de cette politique	1035
Détails de la politique	1035
Version de la politique	1035
Document de politique JSON	1036
En savoir plus	1036

AmazonManagedBlockchainFullAccess	1036
Utilisation de cette politique	1036
Détails de la politique	1037
Version de la politique	1037
Document de politique JSON	1037
En savoir plus	1037
AmazonManagedBlockchainReadOnlyAccess	1038
Utilisation de cette politique	1038
Détails de la politique	1038
Version de la politique	1038
Document de politique JSON	1038
En savoir plus	1039
AmazonManagedBlockchainServiceRolePolicy	1039
Utilisation de cette politique	1039
Détails de la politique	1039
Version de la politique	1039
Document de politique JSON	1040
En savoir plus	1040
AmazonMCSFullAccess	1040
Utilisation de cette politique	1041
Détails de la politique	1041
Version de la politique	1041
Document de politique JSON	1041
En savoir plus	1042
AmazonMCSReadOnlyAccess	1042
Utilisation de cette politique	1043
Détails de la politique	1043
Version de la politique	1043
Document de politique JSON	1043
En savoir plus	1044
AmazonMechanicalTurkFullAccess	1044
Utilisation de cette politique	1044
Détails de la politique	1044
Version de la politique	1044
Document de politique JSON	1045
En savoir plus	1045

AmazonMechanicalTurkReadOnly	1045
Utilisation de cette politique	1045
Détails de la politique	1045
Version de la politique	1046
Document de politique JSON	1046
En savoir plus	1046
AmazonMemoryDBFullAccess	1046
Utilisation de cette politique	1047
Détails de la politique	1047
Version de la politique	1047
Document de politique JSON	1047
En savoir plus	1048
AmazonMemoryDBReadOnlyAccess	1048
Utilisation de cette politique	1048
Détails de la politique	1048
Version de la politique	1048
Document de politique JSON	1049
En savoir plus	1049
AmazonMobileAnalyticsFinancialReportAccess	1049
Utilisation de cette politique	1049
Détails de la politique	1049
Version de la politique	1050
Document de politique JSON	1050
En savoir plus	1050
AmazonMobileAnalyticsFullAccess	1050
Utilisation de cette politique	1051
Détails de la politique	1051
Version de la politique	1051
Document de politique JSON	1051
En savoir plus	1051
AmazonMobileAnalyticsNon-financialReportAccess	1052
Utilisation de cette politique	1052
Détails de la politique	1052
Version de la politique	1052
Document de politique JSON	1052
En savoir plus	1053

AmazonMobileAnalyticsWriteOnlyAccess	1053
Utilisation de cette politique	1053
Détails de la politique	1053
Version de la politique	1053
Document de politique JSON	1054
En savoir plus	1054
AmazonMonitronFullAccess	1054
Utilisation de cette politique	1054
Détails de la politique	1054
Version de la politique	1055
Document de politique JSON	1055
En savoir plus	1057
AmazonMQApiFullAccess	1057
Utilisation de cette politique	1057
Détails de la politique	1057
Version de la politique	1057
Document de politique JSON	1057
En savoir plus	1058
AmazonMQApiReadOnlyAccess	1059
Utilisation de cette politique	1059
Détails de la politique	1059
Version de la politique	1059
Document de politique JSON	1059
En savoir plus	1060
AmazonMQFullAccess	1060
Utilisation de cette politique	1060
Détails de la politique	1060
Version de la politique	1060
Document de politique JSON	1061
En savoir plus	1062
AmazonMQReadOnlyAccess	1062
Utilisation de cette politique	1063
Détails de la politique	1063
Version de la politique	1063
Document de politique JSON	1063
En savoir plus	1064

AmazonMQServiceRolePolicy	1064
Utilisation de cette politique	1064
Détails de la politique	1064
Version de la politique	1064
Document de politique JSON	1064
En savoir plus	1066
AmazonMSKConnectReadOnlyAccess	1066
Utilisation de cette politique	1067
Détails de la politique	1067
Version de la politique	1067
Document de politique JSON	1067
En savoir plus	1068
AmazonMSKFullAccess	1068
Utilisation de cette politique	1068
Détails de la politique	1069
Version de la politique	1069
Document de politique JSON	1069
En savoir plus	1072
AmazonMSKReadOnlyAccess	1072
Utilisation de cette politique	1072
Détails de la politique	1072
Version de la politique	1072
Document de politique JSON	1073
En savoir plus	1073
AmazonMWAAServerlessServiceRolePolicy	1073
Utilisation de cette politique	1074
Détails de la politique	1074
Version de la politique	1074
Document de politique JSON	1074
En savoir plus	1075
AmazonMWAAServiceRolePolicy	1075
Utilisation de cette politique	1075
Détails de la politique	1075
Version de la politique	1075
Document de politique JSON	1076
En savoir plus	1078

AmazonNimbleStudio-LaunchProfileWorker	1078
Utilisation de cette politique	1078
Détails de la politique	1078
Version de la politique	1078
Document de politique JSON	1079
En savoir plus	1079
AmazonNimbleStudio-StudioAdmin	1080
Utilisation de cette politique	1080
Détails de la politique	1080
Version de la politique	1080
Document de politique JSON	1080
En savoir plus	1082
AmazonNimbleStudio-StudioUser	1082
Utilisation de cette politique	1082
Détails de la politique	1083
Version de la politique	1083
Document de politique JSON	1083
En savoir plus	1085
AmazonODBAutonomousDatabaseAdmin	1085
Utilisation de cette politique	1085
Détails de la politique	1085
Version de la politique	1086
Document de politique JSON	1086
En savoir plus	1088
AmazonODBAutonomousVmClusterAdmin	1088
Utilisation de cette politique	1088
Détails de la politique	1088
Version de la politique	1089
Document de politique JSON	1089
En savoir plus	1090
AmazonODBExadataInfrastructureAdmin	1091
Utilisation de cette politique	1091
Détails de la politique	1091
Version de la politique	1091
Document de politique JSON	1091
En savoir plus	1093

AmazonODBExadataVmClusterAdmin	1093
Utilisation de cette politique	1093
Détails de la politique	1093
Version de la politique	1094
Document de politique JSON	1094
En savoir plus	1095
AmazonODBExascaleStorageVaultAdmin	1096
Utilisation de cette politique	1096
Détails de la politique	1096
Version de la politique	1096
Document de politique JSON	1096
En savoir plus	1098
AmazonODBExascaleVmClusterAdmin	1098
Utilisation de cette politique	1098
Détails de la politique	1098
Version de la politique	1099
Document de politique JSON	1099
En savoir plus	1101
AmazonODBFullAccess	1101
Utilisation de cette politique	1101
Détails de la politique	1101
Version de la politique	1101
Document de politique JSON	1101
En savoir plus	1105
AmazonODBNetworkAdmin	1105
Utilisation de cette politique	1105
Détails de la politique	1105
Version de la politique	1105
Document de politique JSON	1105
En savoir plus	1107
AmazonODBReadOnlyAccess	1107
Utilisation de cette politique	1108
Détails de la politique	1108
Version de la politique	1108
Document de politique JSON	1108
En savoir plus	1110

AmazonODBSERVICERolePolicy	1110
Utilisation de cette politique	1110
Détails de la politique	1110
Version de la politique	1110
Document de politique JSON	1110
En savoir plus	1112
AmazonOmicsFullAccess	1112
Utilisation de cette politique	1112
Détails de la politique	1112
Version de la politique	1113
Document de politique JSON	1113
En savoir plus	1114
AmazonOmicsReadOnlyAccess	1114
Utilisation de cette politique	1114
Détails de la politique	1114
Version de la politique	1114
Document de politique JSON	1115
En savoir plus	1115
AmazonOneEnterpriseFullAccess	1115
Utilisation de cette politique	1115
Détails de la politique	1115
Version de la politique	1116
Document de politique JSON	1116
En savoir plus	1116
AmazonOneEnterpriseInstallerAccess	1116
Utilisation de cette politique	1117
Détails de la politique	1117
Version de la politique	1117
Document de politique JSON	1117
En savoir plus	1118
AmazonOneEnterpriseReadOnlyAccess	1118
Utilisation de cette politique	1118
Détails de la politique	1118
Version de la politique	1118
Document de politique JSON	1119
En savoir plus	1119

AmazonOpenSearchDashboardsServiceRolePolicy	1119
Utilisation de cette politique	1119
Détails de la politique	1119
Version de la politique	1120
Document de politique JSON	1120
En savoir plus	1120
AmazonOpenSearchDirectQueryGlueCreateAccess	1121
Utilisation de cette politique	1121
Détails de la politique	1121
Version de la politique	1121
Document de politique JSON	1121
En savoir plus	1122
AmazonOpenSearchIngestionFullAccess	1122
Utilisation de cette politique	1122
Détails de la politique	1122
Version de la politique	1122
Document de politique JSON	1123
En savoir plus	1124
AmazonOpenSearchIngestionReadOnlyAccess	1124
Utilisation de cette politique	1124
Détails de la politique	1124
Version de la politique	1124
Document de politique JSON	1124
En savoir plus	1125
AmazonOpenSearchIngestionServiceRolePolicy	1125
Utilisation de cette politique	1125
Détails de la politique	1125
Version de la politique	1126
Document de politique JSON	1126
En savoir plus	1128
AmazonOpenSearchServerlessServiceRolePolicy	1128
Utilisation de cette politique	1128
Détails de la politique	1128
Version de la politique	1128
Document de politique JSON	1129
En savoir plus	1129

AmazonOpenSearchServiceCognitoAccess	1129
Utilisation de cette politique	1129
Détails de la politique	1129
Version de la politique	1130
Document de politique JSON	1130
En savoir plus	1131
AmazonOpenSearchServiceFullAccess	1131
Utilisation de cette politique	1131
Détails de la politique	1131
Version de la politique	1132
Document de politique JSON	1132
En savoir plus	1132
AmazonOpenSearchServiceReadOnlyAccess	1132
Utilisation de cette politique	1133
Détails de la politique	1133
Version de la politique	1133
Document de politique JSON	1133
En savoir plus	1134
AmazonOpenSearchServiceRolePolicy	1134
Utilisation de cette politique	1134
Détails de la politique	1134
Version de la politique	1134
Document de politique JSON	1135
En savoir plus	1139
AmazonPersonalizeFullAccess	1140
Utilisation de cette politique	1140
Détails de la politique	1140
Version de la politique	1140
Document de politique JSON	1140
En savoir plus	1141
AmazonPollyFullAccess	1142
Utilisation de cette politique	1142
Détails de la politique	1142
Version de la politique	1142
Document de politique JSON	1142
En savoir plus	1143

AmazonPollyReadOnlyAccess	1143
Utilisation de cette politique	1143
Détails de la politique	1143
Version de la politique	1143
Document de politique JSON	1143
En savoir plus	1144
AmazonPrometheusConsoleFullAccess	1144
Utilisation de cette politique	1144
Détails de la politique	1145
Version de la politique	1145
Document de politique JSON	1145
En savoir plus	1146
AmazonPrometheusFullAccess	1146
Utilisation de cette politique	1146
Détails de la politique	1147
Version de la politique	1147
Document de politique JSON	1147
En savoir plus	1148
AmazonPrometheusQueryAccess	1148
Utilisation de cette politique	1148
Détails de la politique	1148
Version de la politique	1149
Document de politique JSON	1149
En savoir plus	1149
AmazonPrometheusRemoteWriteAccess	1150
Utilisation de cette politique	1150
Détails de la politique	1150
Version de la politique	1150
Document de politique JSON	1150
En savoir plus	1151
AmazonPrometheusScraperServiceRolePolicy	1151
Utilisation de cette politique	1151
Détails de la politique	1151
Version de la politique	1151
Document de politique JSON	1152
En savoir plus	1154

AmazonQDeveloperAccess	1154
Utilisation de cette politique	1155
Détails de la politique	1155
Version de la politique	1155
Document de politique JSON	1155
En savoir plus	1156
AmazonQFullAccess	1157
Utilisation de cette politique	1157
Détails de la politique	1157
Version de la politique	1157
Document de politique JSON	1157
En savoir plus	1159
AmazonQLDBConsoleFullAccess	1159
Utilisation de cette politique	1159
Détails de la politique	1160
Version de la politique	1160
Document de politique JSON	1160
En savoir plus	1162
AmazonQLDBFullAccess	1162
Utilisation de cette politique	1162
Détails de la politique	1162
Version de la politique	1162
Document de politique JSON	1163
En savoir plus	1164
AmazonQLDBReadOnly	1164
Utilisation de cette politique	1164
Détails de la politique	1164
Version de la politique	1165
Document de politique JSON	1165
En savoir plus	1165
AmazonRDSBetaServiceRolePolicy	1166
Utilisation de cette politique	1166
Détails de la politique	1166
Version de la politique	1166
Document de politique JSON	1166
En savoir plus	1169

AmazonRDSCustomInstanceProfileRolePolicy	1169
Utilisation de cette politique	1170
Détails de la politique	1170
Version de la politique	1170
Document de politique JSON	1170
En savoir plus	1177
AmazonRDSCustomPreviewServiceRolePolicy	1177
Utilisation de cette politique	1178
Détails de la politique	1178
Version de la politique	1178
Document de politique JSON	1178
En savoir plus	1196
AmazonRDSCustomServiceRolePolicy	1196
Utilisation de cette politique	1196
Détails de la politique	1196
Version de la politique	1196
Document de politique JSON	1196
En savoir plus	1215
AmazonRDSDDataFullAccess	1216
Utilisation de cette politique	1216
Détails de la politique	1216
Version de la politique	1216
Document de politique JSON	1216
En savoir plus	1217
AmazonRDSDirectoryServiceAccess	1218
Utilisation de cette politique	1218
Détails de la politique	1218
Version de la politique	1218
Document de politique JSON	1218
En savoir plus	1219
AmazonRDSEnhancedMonitoringRole	1219
Utilisation de cette politique	1219
Détails de la politique	1219
Version de la politique	1219
Document de politique JSON	1220
En savoir plus	1220

AmazonRDSFullAccess	1221
Utilisation de cette politique	1221
Détails de la politique	1221
Version de la politique	1221
Document de politique JSON	1221
En savoir plus	1223
AmazonRDSPerformanceInsightsFullAccess	1223
Utilisation de cette politique	1224
Détails de la politique	1224
Version de la politique	1224
Document de politique JSON	1224
En savoir plus	1226
AmazonRDSPerformanceInsightsReadOnly	1226
Utilisation de cette politique	1226
Détails de la politique	1226
Version de la politique	1226
Document de politique JSON	1227
En savoir plus	1229
AmazonRDSPreviewServiceRolePolicy	1229
Utilisation de cette politique	1229
Détails de la politique	1229
Version de la politique	1230
Document de politique JSON	1230
En savoir plus	1233
AmazonRDSReadOnlyAccess	1233
Utilisation de cette politique	1233
Détails de la politique	1233
Version de la politique	1233
Document de politique JSON	1234
En savoir plus	1235
AmazonRDSServiceRolePolicy	1235
Utilisation de cette politique	1235
Détails de la politique	1235
Version de la politique	1235
Document de politique JSON	1236
En savoir plus	1239

AmazonRedshiftAllCommandsFullAccess	1240
Utilisation de cette politique	1240
Détails de la politique	1240
Version de la politique	1240
Document de politique JSON	1240
En savoir plus	1246
AmazonRedshiftDataFullAccess	1246
Utilisation de cette politique	1246
Détails de la politique	1246
Version de la politique	1246
Document de politique JSON	1246
En savoir plus	1248
AmazonRedshiftFederatedAuthorization	1249
Utilisation de cette politique	1249
Détails de la politique	1249
Version de la politique	1249
Document de politique JSON	1249
En savoir plus	1250
AmazonRedshiftFullAccess	1251
Utilisation de cette politique	1251
Détails de la politique	1251
Version de la politique	1251
Document de politique JSON	1251
En savoir plus	1253
AmazonRedshiftQueryEditor	1253
Utilisation de cette politique	1254
Détails de la politique	1254
Version de la politique	1254
Document de politique JSON	1254
En savoir plus	1256
AmazonRedshiftQueryEditorV2FullAccess	1256
Utilisation de cette politique	1256
Détails de la politique	1257
Version de la politique	1257
Document de politique JSON	1257
En savoir plus	1258

AmazonRedshiftQueryEditorV2NoSharing	1259
Utilisation de cette politique	1259
Détails de la politique	1259
Version de la politique	1259
Document de politique JSON	1259
En savoir plus	1263
AmazonRedshiftQueryEditorV2ReadSharing	1263
Utilisation de cette politique	1263
Détails de la politique	1264
Version de la politique	1264
Document de politique JSON	1264
En savoir plus	1269
AmazonRedshiftQueryEditorV2ReadWriteSharing	1269
Utilisation de cette politique	1269
Détails de la politique	1269
Version de la politique	1270
Document de politique JSON	1270
En savoir plus	1275
AmazonRedshiftReadOnlyAccess	1275
Utilisation de cette politique	1275
Détails de la politique	1275
Version de la politique	1275
Document de politique JSON	1276
En savoir plus	1276
AmazonRedshiftServiceLinkedRolePolicy	1277
Utilisation de cette politique	1277
Détails de la politique	1277
Version de la politique	1277
Document de politique JSON	1277
En savoir plus	1284
AmazonRekognitionCustomLabelsFullAccess	1284
Utilisation de cette politique	1284
Détails de la politique	1284
Version de la politique	1284
Document de politique JSON	1284
En savoir plus	1286

AmazonRekognitionFullAccess	1286
Utilisation de cette politique	1286
Détails de la politique	1286
Version de la politique	1286
Document de politique JSON	1286
En savoir plus	1287
AmazonRekognitionReadOnlyAccess	1287
Utilisation de cette politique	1287
Détails de la politique	1287
Version de la politique	1288
Document de politique JSON	1288
En savoir plus	1289
AmazonRekognitionServiceRole	1289
Utilisation de cette politique	1289
Détails de la politique	1289
Version de la politique	1290
Document de politique JSON	1290
En savoir plus	1290
AmazonRoute53AutoNamingFullAccess	1291
Utilisation de cette politique	1291
Détails de la politique	1291
Version de la politique	1291
Document de politique JSON	1291
En savoir plus	1292
AmazonRoute53AutoNamingReadOnlyAccess	1292
Utilisation de cette politique	1292
Détails de la politique	1293
Version de la politique	1293
Document de politique JSON	1293
En savoir plus	1293
AmazonRoute53AutoNamingRegistrantAccess	1294
Utilisation de cette politique	1294
Détails de la politique	1294
Version de la politique	1294
Document de politique JSON	1294
En savoir plus	1295

AmazonRoute53DomainsFullAccess	1295
Utilisation de cette politique	1295
Détails de la politique	1295
Version de la politique	1296
Document de politique JSON	1296
En savoir plus	1296
AmazonRoute53DomainsReadOnlyAccess	1297
Utilisation de cette politique	1297
Détails de la politique	1297
Version de la politique	1297
Document de politique JSON	1297
En savoir plus	1298
AmazonRoute53FullAccess	1298
Utilisation de cette politique	1298
Détails de la politique	1298
Version de la politique	1298
Document de politique JSON	1299
En savoir plus	1300
AmazonRoute53GlobalResolverFullAccess	1300
Utilisation de cette politique	1300
Détails de la politique	1300
Version de la politique	1300
Document de politique JSON	1300
En savoir plus	1302
AmazonRoute53GlobalResolverReadOnlyAccess	1302
Utilisation de cette politique	1302
Détails de la politique	1303
Version de la politique	1303
Document de politique JSON	1303
En savoir plus	1304
AmazonRoute53ProfilesFullAccess	1304
Utilisation de cette politique	1304
Détails de la politique	1304
Version de la politique	1304
Document de politique JSON	1305
En savoir plus	1306

AmazonRoute53ProfilesReadOnlyAccess	1306
Utilisation de cette politique	1306
Détails de la politique	1306
Version de la politique	1306
Document de politique JSON	1306
En savoir plus	1307
AmazonRoute53ReadOnlyAccess	1307
Utilisation de cette politique	1308
Détails de la politique	1308
Version de la politique	1308
Document de politique JSON	1308
En savoir plus	1309
AmazonRoute53RecoveryClusterFullAccess	1309
Utilisation de cette politique	1309
Détails de la politique	1309
Version de la politique	1309
Document de politique JSON	1309
En savoir plus	1310
AmazonRoute53RecoveryClusterReadOnlyAccess	1310
Utilisation de cette politique	1310
Détails de la politique	1310
Version de la politique	1311
Document de politique JSON	1311
En savoir plus	1311
AmazonRoute53RecoveryControlConfigFullAccess	1311
Utilisation de cette politique	1312
Détails de la politique	1312
Version de la politique	1312
Document de politique JSON	1312
En savoir plus	1312
AmazonRoute53RecoveryControlConfigReadOnlyAccess	1313
Utilisation de cette politique	1313
Détails de la politique	1313
Version de la politique	1313
Document de politique JSON	1313
En savoir plus	1314

AmazonRoute53RecoveryReadinessFullAccess	1314
Utilisation de cette politique	1314
Détails de la politique	1314
Version de la politique	1315
Document de politique JSON	1315
En savoir plus	1315
AmazonRoute53RecoveryReadinessReadOnlyAccess	1315
Utilisation de cette politique	1316
Détails de la politique	1316
Version de la politique	1316
Document de politique JSON	1316
En savoir plus	1317
AmazonRoute53ResolverFullAccess	1317
Utilisation de cette politique	1317
Détails de la politique	1317
Version de la politique	1318
Document de politique JSON	1318
En savoir plus	1318
AmazonRoute53ResolverReadOnlyAccess	1319
Utilisation de cette politique	1319
Détails de la politique	1319
Version de la politique	1319
Document de politique JSON	1319
En savoir plus	1320
AmazonS3ExpressFullAccess	1320
Utilisation de cette politique	1320
Détails de la politique	1320
Version de la politique	1321
Document de politique JSON	1321
En savoir plus	1321
AmazonS3ExpressReadOnlyAccess	1321
Utilisation de cette politique	1322
Détails de la politique	1322
Version de la politique	1322
Document de politique JSON	1322
En savoir plus	1323

AmazonS3FilesClientFullAccess	1323
Utilisation de cette politique	1323
Détails de la politique	1323
Version de la politique	1324
Document de politique JSON	1324
En savoir plus	1324
AmazonS3FilesClientReadOnlyAccess	1324
Utilisation de cette politique	1325
Détails de la politique	1325
Version de la politique	1325
Document de politique JSON	1325
En savoir plus	1325
AmazonS3FilesClientReadWriteAccess	1326
Utilisation de cette politique	1326
Détails de la politique	1326
Version de la politique	1326
Document de politique JSON	1326
En savoir plus	1327
AmazonS3FilesCSIDriverPolicy	1327
Utilisation de cette politique	1327
Détails de la politique	1327
Version de la politique	1327
Document de politique JSON	1328
En savoir plus	1329
AmazonS3FilesFullAccess	1329
Utilisation de cette politique	1329
Détails de la politique	1330
Version de la politique	1330
Document de politique JSON	1330
En savoir plus	1332
AmazonS3FilesReadOnlyAccess	1332
Utilisation de cette politique	1332
Détails de la politique	1332
Version de la politique	1332
Document de politique JSON	1333
En savoir plus	1333

AmazonS3FullAccess	1334
Utilisation de cette politique	1334
Détails de la politique	1334
Version de la politique	1334
Document de politique JSON	1334
En savoir plus	1335
AmazonS3ObjectLambdaExecutionRolePolicy	1335
Utilisation de cette politique	1335
Détails de la politique	1335
Version de la politique	1335
Document de politique JSON	1336
En savoir plus	1336
AmazonS3OutpostsFullAccess	1336
Utilisation de cette politique	1336
Détails de la politique	1337
Version de la politique	1337
Document de politique JSON	1337
En savoir plus	1338
AmazonS3OutpostsReadOnlyAccess	1338
Utilisation de cette politique	1338
Détails de la politique	1338
Version de la politique	1339
Document de politique JSON	1339
En savoir plus	1340
AmazonS3ReadOnlyAccess	1340
Utilisation de cette politique	1340
Détails de la politique	1340
Version de la politique	1341
Document de politique JSON	1341
En savoir plus	1341
AmazonS3TablesFullAccess	1341
Utilisation de cette politique	1342
Détails de la politique	1342
Version de la politique	1342
Document de politique JSON	1342
En savoir plus	1343

AmazonS3TablesLakeFormationServiceRole	1343
Utilisation de cette politique	1343
Détails de la politique	1343
Version de la politique	1344
Document de politique JSON	1344
En savoir plus	1346
AmazonS3TablesReadOnlyAccess	1346
Utilisation de cette politique	1346
Détails de la politique	1346
Version de la politique	1347
Document de politique JSON	1347
En savoir plus	1347
AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy	1347
Utilisation de cette politique	1348
Détails de la politique	1348
Version de la politique	1348
Document de politique JSON	1348
En savoir plus	1360
AmazonSageMakerCanvasAIServicesAccess	1360
Utilisation de cette politique	1360
Détails de la politique	1360
Version de la politique	1360
Document de politique JSON	1361
En savoir plus	1364
AmazonSageMakerCanvasBedrockAccess	1364
Utilisation de cette politique	1364
Détails de la politique	1364
Version de la politique	1364
Document de politique JSON	1364
En savoir plus	1365
AmazonSageMakerCanvasDataPrepFullAccess	1365
Utilisation de cette politique	1366
Détails de la politique	1366
Version de la politique	1366
Document de politique JSON	1366
En savoir plus	1376

AmazonSageMakerCanvasDirectDeployAccess	1376
Utilisation de cette politique	1376
Détails de la politique	1376
Version de la politique	1376
Document de politique JSON	1377
En savoir plus	1377
AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy	1378
Utilisation de cette politique	1378
Détails de la politique	1378
Version de la politique	1378
Document de politique JSON	1378
En savoir plus	1380
AmazonSageMakerCanvasForecastAccess	1380
Utilisation de cette politique	1380
Détails de la politique	1380
Version de la politique	1380
Document de politique JSON	1381
En savoir plus	1381
AmazonSageMakerCanvasFullAccess	1381
Utilisation de cette politique	1382
Détails de la politique	1382
Version de la politique	1382
Document de politique JSON	1382
En savoir plus	1394
AmazonSageMakerCanvasSMDDataScienceAssistantAccess	1395
Utilisation de cette politique	1395
Détails de la politique	1395
Version de la politique	1395
Document de politique JSON	1395
En savoir plus	1396
AmazonSageMakerCapacityReservationServiceRolePolicy	1396
Utilisation de cette politique	1397
Détails de la politique	1397
Version de la politique	1397
Document de politique JSON	1397
En savoir plus	1398

AmazonSageMakerClusterInstanceRolePolicy	1398
Utilisation de cette politique	1398
Détails de la politique	1398
Version de la politique	1398
Document de politique JSON	1398
En savoir plus	1400
AmazonSageMakerCoreServiceRolePolicy	1400
Utilisation de cette politique	1401
Détails de la politique	1401
Version de la politique	1401
Document de politique JSON	1401
En savoir plus	1402
AmazonSageMakerEdgeDeviceFleetPolicy	1402
Utilisation de cette politique	1402
Détails de la politique	1402
Version de la politique	1403
Document de politique JSON	1403
En savoir plus	1405
AmazonSageMakerFeatureStoreAccess	1405
Utilisation de cette politique	1405
Détails de la politique	1405
Version de la politique	1405
Document de politique JSON	1406
En savoir plus	1407
AmazonSageMakerFullAccess	1407
Utilisation de cette politique	1407
Détails de la politique	1407
Version de la politique	1407
Document de politique JSON	1407
En savoir plus	1424
AmazonSageMakerGeospatialExecutionRole	1424
Utilisation de cette politique	1424
Détails de la politique	1424
Version de la politique	1425
Document de politique JSON	1425
En savoir plus	1426

AmazonSageMakerGeospatialFullAccess	1426
Utilisation de cette politique	1426
Détails de la politique	1426
Version de la politique	1426
Document de politique JSON	1427
En savoir plus	1427
AmazonSageMakerGroundTruthExecution	1427
Utilisation de cette politique	1428
Détails de la politique	1428
Version de la politique	1428
Document de politique JSON	1428
En savoir plus	1432
AmazonSageMakerHyperPodGatedModelAccess	1432
Utilisation de cette politique	1432
Détails de la politique	1432
Version de la politique	1432
Document de politique JSON	1433
En savoir plus	1433
AmazonSageMakerHyperPodInferenceAccess	1433
Utilisation de cette politique	1434
Détails de la politique	1434
Version de la politique	1434
Document de politique JSON	1434
En savoir plus	1443
AmazonSageMakerHyperPodInferenceGatewayAccess	1443
Utilisation de cette politique	1443
Détails de la politique	1443
Version de la politique	1444
Document de politique JSON	1444
En savoir plus	1445
AmazonSageMakerHyperPodObservabilityAdminAccess	1445
Utilisation de cette politique	1446
Détails de la politique	1446
Version de la politique	1446
Document de politique JSON	1446
En savoir plus	1452

AmazonSageMakerHyperPodServiceRolePolicy	1453
Utilisation de cette politique	1453
Détails de la politique	1453
Version de la politique	1453
Document de politique JSON	1453
En savoir plus	1454
AmazonSageMakerHyperPodTrainingOperatorAccess	1455
Utilisation de cette politique	1455
Détails de la politique	1455
Version de la politique	1455
Document de politique JSON	1455
En savoir plus	1456
AmazonSageMakerInferenceServiceRolePolicy	1456
Utilisation de cette politique	1456
Détails de la politique	1456
Version de la politique	1457
Document de politique JSON	1457
En savoir plus	1459
AmazonSageMakerJobFullAccess	1460
Utilisation de cette politique	1460
Détails de la politique	1460
Version de la politique	1460
Document de politique JSON	1460
En savoir plus	1465
AmazonSageMakerJobRuntimeAccess	1465
Utilisation de cette politique	1465
Détails de la politique	1465
Version de la politique	1466
Document de politique JSON	1466
En savoir plus	1467
AmazonSageMakerMechanicalTurkAccess	1467
Utilisation de cette politique	1468
Détails de la politique	1468
Version de la politique	1468
Document de politique JSON	1468
En savoir plus	1468

AmazonSageMakerModelCustomizationCoreAccess	1469
Utilisation de cette politique	1469
Détails de la politique	1469
Version de la politique	1469
Document de politique JSON	1469
En savoir plus	1481
AmazonSageMakerModelGovernanceUseAccess	1481
Utilisation de cette politique	1482
Détails de la politique	1482
Version de la politique	1482
Document de politique JSON	1482
En savoir plus	1484
AmazonSageMakerModelRegistryFullAccess	1484
Utilisation de cette politique	1484
Détails de la politique	1484
Version de la politique	1485
Document de politique JSON	1485
En savoir plus	1488
AmazonSageMakerNotebooksServiceRolePolicy	1489
Utilisation de cette politique	1489
Détails de la politique	1489
Version de la politique	1489
Document de politique JSON	1489
En savoir plus	1494
AmazonSageMakerPartnerAppsFullAccess	1495
Utilisation de cette politique	1495
Détails de la politique	1495
Version de la politique	1495
Document de politique JSON	1495
En savoir plus	1496
AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy	1496
Utilisation de cette politique	1496
Détails de la politique	1497
Version de la politique	1497
Document de politique JSON	1497
En savoir plus	1498

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy	1498
Utilisation de cette politique	1498
Détails de la politique	1498
Version de la politique	1499
Document de politique JSON	1499
En savoir plus	1502
AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy	1503
Utilisation de cette politique	1503
Détails de la politique	1503
Version de la politique	1503
Document de politique JSON	1503
En savoir plus	1504
AmazonSageMakerPipelinesIntegrations	1504
Utilisation de cette politique	1504
Détails de la politique	1504
Version de la politique	1505
Document de politique JSON	1505
En savoir plus	1507
AmazonSageMakerQuickSightVPCPolicy	1507
Utilisation de cette politique	1507
Détails de la politique	1507
Version de la politique	1507
Document de politique JSON	1508
En savoir plus	1509
AmazonSageMakerReadOnly	1509
Utilisation de cette politique	1509
Détails de la politique	1510
Version de la politique	1510
Document de politique JSON	1510
En savoir plus	1511
AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy	1511
Utilisation de cette politique	1512
Détails de la politique	1512
Version de la politique	1512
Document de politique JSON	1512
En savoir plus	1513

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy	1513
Utilisation de cette politique	1513
Détails de la politique	1513
Version de la politique	1514
Document de politique JSON	1514
En savoir plus	1521
AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy	1521
Utilisation de cette politique	1521
Détails de la politique	1521
Version de la politique	1521
Document de politique JSON	1522
En savoir plus	1532
AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy	1532
Utilisation de cette politique	1532
Détails de la politique	1532
Version de la politique	1533
Document de politique JSON	1533
En savoir plus	1536
AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy	1536
Utilisation de cette politique	1536
Détails de la politique	1536
Version de la politique	1536
Document de politique JSON	1537
En savoir plus	1537
AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy	1537
Utilisation de cette politique	1537
Détails de la politique	1538
Version de la politique	1538
Document de politique JSON	1538
En savoir plus	1538
AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy	1539
Utilisation de cette politique	1539
Détails de la politique	1539
Version de la politique	1539
Document de politique JSON	1539
En savoir plus	1541

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy	1542
Utilisation de cette politique	1542
Détails de la politique	1542
Version de la politique	1542
Document de politique JSON	1542
En savoir plus	1552
AmazonSageMakerSpacesControllerPolicy	1553
Utilisation de cette politique	1553
Détails de la politique	1553
Version de la politique	1553
Document de politique JSON	1553
En savoir plus	1558
AmazonSageMakerSpacesRouterPolicy	1558
Utilisation de cette politique	1558
Détails de la politique	1558
Version de la politique	1559
Document de politique JSON	1559
En savoir plus	1560
AmazonSageMakerTrainingPlanCreateAccess	1560
Utilisation de cette politique	1560
Détails de la politique	1560
Version de la politique	1560
Document de politique JSON	1561
En savoir plus	1562
AmazonSecurityLakeAdministrator	1562
Utilisation de cette politique	1563
Détails de la politique	1563
Version de la politique	1563
Document de politique JSON	1563
En savoir plus	1574
AmazonSecurityLakeMetastoreManager	1574
Utilisation de cette politique	1575
Détails de la politique	1575
Version de la politique	1575
Document de politique JSON	1575
En savoir plus	1577

AmazonSecurityLakePermissionsBoundary	1578
Utilisation de cette politique	1578
Détails de la politique	1578
Version de la politique	1578
Document de politique JSON	1578
En savoir plus	1581
AmazonSESEFullAccess	1582
Utilisation de cette politique	1582
Détails de la politique	1582
Version de la politique	1582
Document de politique JSON	1582
En savoir plus	1583
AmazonSESReadOnlyAccess	1583
Utilisation de cette politique	1583
Détails de la politique	1583
Version de la politique	1583
Document de politique JSON	1584
En savoir plus	1584
AmazonSESServiceRolePolicy	1584
Utilisation de cette politique	1584
Détails de la politique	1585
Version de la politique	1585
Document de politique JSON	1585
En savoir plus	1586
AmazonSNSFullAccess	1586
Utilisation de cette politique	1586
Détails de la politique	1586
Version de la politique	1586
Document de politique JSON	1586
En savoir plus	1587
AmazonSNSReadOnlyAccess	1587
Utilisation de cette politique	1588
Détails de la politique	1588
Version de la politique	1588
Document de politique JSON	1588
En savoir plus	1589

AmazonSNSRole	1589
Utilisation de cette politique	1589
Détails de la politique	1590
Version de la politique	1590
Document de politique JSON	1590
En savoir plus	1590
AmazonSQSFullAccess	1591
Utilisation de cette politique	1591
Détails de la politique	1591
Version de la politique	1591
Document de politique JSON	1591
En savoir plus	1592
AmazonSQSReadOnlyAccess	1592
Utilisation de cette politique	1592
Détails de la politique	1592
Version de la politique	1592
Document de politique JSON	1593
En savoir plus	1593
AmazonSSMAutomationApproverAccess	1593
Utilisation de cette politique	1593
Détails de la politique	1594
Version de la politique	1594
Document de politique JSON	1594
En savoir plus	1594
AmazonSSMAutomationRole	1595
Utilisation de cette politique	1595
Détails de la politique	1595
Version de la politique	1595
Document de politique JSON	1595
En savoir plus	1597
AmazonSSMDirectoryServiceAccess	1597
Utilisation de cette politique	1597
Détails de la politique	1597
Version de la politique	1598
Document de politique JSON	1598
En savoir plus	1598

AmazonSSMFullAccess	1598
Utilisation de cette politique	1599
Détails de la politique	1599
Version de la politique	1599
Document de politique JSON	1599
En savoir plus	1600
AmazonSSMMaintenanceWindowRole	1601
Utilisation de cette politique	1601
Détails de la politique	1601
Version de la politique	1601
Document de politique JSON	1601
En savoir plus	1603
AmazonSSMManagedEC2InstanceDefaultPolicy	1603
Utilisation de cette politique	1603
Détails de la politique	1603
Version de la politique	1603
Document de politique JSON	1604
En savoir plus	1605
AmazonSSMManagedInstanceCore	1605
Utilisation de cette politique	1605
Détails de la politique	1605
Version de la politique	1605
Document de politique JSON	1606
En savoir plus	1607
AmazonSSMPatchAssociation	1607
Utilisation de cette politique	1607
Détails de la politique	1607
Version de la politique	1608
Document de politique JSON	1608
En savoir plus	1608
AmazonSSMReadOnlyAccess	1609
Utilisation de cette politique	1609
Détails de la politique	1609
Version de la politique	1609
Document de politique JSON	1609
En savoir plus	1610

AmazonSSMServiceRolePolicy	1610
Utilisation de cette politique	1610
Détails de la politique	1610
Version de la politique	1610
Document de politique JSON	1611
En savoir plus	1616
AmazonSumerianFullAccess	1616
Utilisation de cette politique	1616
Détails de la politique	1617
Version de la politique	1617
Document de politique JSON	1617
En savoir plus	1617
AmazonTextractFullAccess	1618
Utilisation de cette politique	1618
Détails de la politique	1618
Version de la politique	1618
Document de politique JSON	1618
En savoir plus	1619
AmazonTextractServiceRole	1619
Utilisation de cette politique	1619
Détails de la politique	1619
Version de la politique	1619
Document de politique JSON	1619
En savoir plus	1620
AmazonTimestreamConsoleFullAccess	1620
Utilisation de cette politique	1620
Détails de la politique	1620
Version de la politique	1621
Document de politique JSON	1621
En savoir plus	1623
AmazonTimestreamFullAccess	1624
Utilisation de cette politique	1624
Détails de la politique	1624
Version de la politique	1624
Document de politique JSON	1624
En savoir plus	1625

AmazonTimestreamInfluxDBFullAccess	1626
Utilisation de cette politique	1626
Détails de la politique	1626
Version de la politique	1626
Document de politique JSON	1626
En savoir plus	1629
AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess	1629
Utilisation de cette politique	1629
Détails de la politique	1630
Version de la politique	1630
Document de politique JSON	1630
En savoir plus	1632
AmazonTimestreamInfluxDBServiceRolePolicy	1632
Utilisation de cette politique	1633
Détails de la politique	1633
Version de la politique	1633
Document de politique JSON	1633
En savoir plus	1636
AmazonTimestreamReadOnlyAccess	1637
Utilisation de cette politique	1637
Détails de la politique	1637
Version de la politique	1637
Document de politique JSON	1637
En savoir plus	1638
AmazonTranscribeFullAccess	1638
Utilisation de cette politique	1638
Détails de la politique	1638
Version de la politique	1639
Document de politique JSON	1639
En savoir plus	1639
AmazonTranscribeReadOnlyAccess	1640
Utilisation de cette politique	1640
Détails de la politique	1640
Version de la politique	1640
Document de politique JSON	1640
En savoir plus	1641

AmazonVerifiedPermissionsFullAccess	1641
Utilisation de cette politique	1641
Détails de la politique	1641
Version de la politique	1641
Document de politique JSON	1642
En savoir plus	1642
AmazonVerifiedPermissionsReadOnlyAccess	1642
Utilisation de cette politique	1643
Détails de la politique	1643
Version de la politique	1643
Document de politique JSON	1643
En savoir plus	1644
AmazonVPCCrossAccountNetworkInterfaceOperations	1644
Utilisation de cette politique	1644
Détails de la politique	1644
Version de la politique	1645
Document de politique JSON	1645
En savoir plus	1646
AmazonVPCFullAccess	1646
Utilisation de cette politique	1647
Détails de la politique	1647
Version de la politique	1647
Document de politique JSON	1647
En savoir plus	1651
AmazonVPCNetworkAccessAnalyzerFullAccessPolicy	1651
Utilisation de cette politique	1651
Détails de la politique	1651
Version de la politique	1652
Document de politique JSON	1652
En savoir plus	1655
AmazonVPCReachabilityAnalyzerFullAccessPolicy	1656
Utilisation de cette politique	1656
Détails de la politique	1656
Version de la politique	1656
Document de politique JSON	1656
En savoir plus	1659

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy	1660
Utilisation de cette politique	1660
Détails de la politique	1660
Version de la politique	1660
Document de politique JSON	1660
En savoir plus	1661
AmazonVPCReadOnlyAccess	1661
Utilisation de cette politique	1661
Détails de la politique	1661
Version de la politique	1661
Document de politique JSON	1662
En savoir plus	1663
AmazonWorkDocsFullAccess	1663
Utilisation de cette politique	1663
Détails de la politique	1663
Version de la politique	1664
Document de politique JSON	1664
En savoir plus	1664
AmazonWorkDocsReadOnlyAccess	1664
Utilisation de cette politique	1665
Détails de la politique	1665
Version de la politique	1665
Document de politique JSON	1665
En savoir plus	1666
AmazonWorkMailEventsServiceRolePolicy	1666
Utilisation de cette politique	1666
Détails de la politique	1666
Version de la politique	1666
Document de politique JSON	1667
En savoir plus	1667
AmazonWorkMailFullAccess	1667
Utilisation de cette politique	1667
Détails de la politique	1667
Version de la politique	1668
Document de politique JSON	1668
En savoir plus	1670

AmazonWorkMailMessageFlowFullAccess	1670
Utilisation de cette politique	1670
Détails de la politique	1670
Version de la politique	1670
Document de politique JSON	1671
En savoir plus	1671
AmazonWorkMailMessageFlowReadOnlyAccess	1671
Utilisation de cette politique	1671
Détails de la politique	1671
Version de la politique	1672
Document de politique JSON	1672
En savoir plus	1672
AmazonWorkMailReadOnlyAccess	1672
Utilisation de cette politique	1673
Détails de la politique	1673
Version de la politique	1673
Document de politique JSON	1673
En savoir plus	1674
AmazonWorkSpacesAdmin	1674
Utilisation de cette politique	1674
Détails de la politique	1674
Version de la politique	1674
Document de politique JSON	1675
En savoir plus	1676
AmazonWorkSpacesApplicationManagerAdminAccess	1676
Utilisation de cette politique	1676
Détails de la politique	1676
Version de la politique	1676
Document de politique JSON	1677
En savoir plus	1677
AmazonWorkspacesPCAAccess	1677
Utilisation de cette politique	1677
Détails de la politique	1677
Version de la politique	1678
Document de politique JSON	1678
En savoir plus	1678

AmazonWorkSpacesPoolServiceAccess	1679
Utilisation de cette politique	1679
Détails de la politique	1679
Version de la politique	1679
Document de politique JSON	1679
En savoir plus	1681
AmazonWorkSpacesSecureBrowserReadOnly	1681
Utilisation de cette politique	1681
Détails de la politique	1681
Version de la politique	1681
Document de politique JSON	1681
En savoir plus	1683
AmazonWorkSpacesSelfServiceAccess	1683
Utilisation de cette politique	1683
Détails de la politique	1683
Version de la politique	1683
Document de politique JSON	1683
En savoir plus	1684
AmazonWorkSpacesServiceAccess	1684
Utilisation de cette politique	1684
Détails de la politique	1684
Version de la politique	1685
Document de politique JSON	1685
En savoir plus	1685
AmazonWorkSpacesThinClientFullAccess	1685
Utilisation de cette politique	1686
Détails de la politique	1686
Version de la politique	1686
Document de politique JSON	1686
En savoir plus	1687
AmazonWorkSpacesThinClientMonitoringServiceRolePolicy	1688
Utilisation de cette politique	1688
Détails de la politique	1688
Version de la politique	1688
Document de politique JSON	1688
En savoir plus	1689

AmazonWorkSpacesThinClientReadOnlyAccess	1689
Utilisation de cette politique	1689
Détails de la politique	1689
Version de la politique	1690
Document de politique JSON	1690
En savoir plus	1691
AmazonWorkSpacesWebReadOnly	1691
Utilisation de cette politique	1691
Détails de la politique	1691
Version de la politique	1692
Document de politique JSON	1692
En savoir plus	1693
AmazonWorkSpacesWebServiceRolePolicy	1693
Utilisation de cette politique	1693
Détails de la politique	1693
Version de la politique	1694
Document de politique JSON	1694
En savoir plus	1696
AmazonZocaloFullAccess	1696
Utilisation de cette politique	1696
Détails de la politique	1696
Version de la politique	1697
Document de politique JSON	1697
En savoir plus	1697
AmazonZocaloReadOnlyAccess	1698
Utilisation de cette politique	1698
Détails de la politique	1698
Version de la politique	1698
Document de politique JSON	1698
En savoir plus	1699
AmplifyBackendDeployFullAccess	1699
Utilisation de cette politique	1699
Détails de la politique	1699
Version de la politique	1699
Document de politique JSON	1700
En savoir plus	1704

AnthropicFullAccess	1704
Utilisation de cette politique	1704
Détails de la politique	1704
Version de la politique	1705
Document de politique JSON	1705
En savoir plus	1707
AnthropicLimitedAccess	1707
Utilisation de cette politique	1707
Détails de la politique	1707
Version de la politique	1707
Document de politique JSON	1707
En savoir plus	1710
AnthropicReadOnlyAccess	1710
Utilisation de cette politique	1710
Détails de la politique	1710
Version de la politique	1710
Document de politique JSON	1711
En savoir plus	1712
AnthropicSelfHostedEnvironmentAccess	1712
Utilisation de cette politique	1712
Détails de la politique	1713
Version de la politique	1713
Document de politique JSON	1713
En savoir plus	1714
APIGatewayServiceRolePolicy	1714
Utilisation de cette politique	1714
Détails de la politique	1714
Version de la politique	1714
Document de politique JSON	1715
En savoir plus	1717
AppIntegrationsServiceLinkedRolePolicy	1717
Utilisation de cette politique	1717
Détails de la politique	1717
Version de la politique	1717
Document de politique JSON	1718
En savoir plus	1719

ApplicationAutoScalingForAmazonAppStreamAccess	1719
Utilisation de cette politique	1720
Détails de la politique	1720
Version de la politique	1720
Document de politique JSON	1720
En savoir plus	1721
ApplicationDiscoveryServiceContinuousExportServiceRolePolicy	1721
Utilisation de cette politique	1721
Détails de la politique	1721
Version de la politique	1722
Document de politique JSON	1722
En savoir plus	1724
AppRunnerNetworkingServiceRolePolicy	1724
Utilisation de cette politique	1724
Détails de la politique	1724
Version de la politique	1724
Document de politique JSON	1725
En savoir plus	1726
AppRunnerServiceRolePolicy	1726
Utilisation de cette politique	1726
Détails de la politique	1726
Version de la politique	1726
Document de politique JSON	1727
En savoir plus	1728
AppStudioServiceRolePolicy	1728
Utilisation de cette politique	1728
Détails de la politique	1728
Version de la politique	1728
Document de politique JSON	1728
En savoir plus	1731
AssuranceServiceRolePolicy	1731
Utilisation de cette politique	1731
Détails de la politique	1731
Version de la politique	1731
Document de politique JSON	1731
En savoir plus	1742

AuroraDsqlServiceLinkedRolePolicy	1742
Utilisation de cette politique	1742
Détails de la politique	1742
Version de la politique	1743
Document de politique JSON	1743
En savoir plus	1743
AutoScalingConsoleFullAccess	1744
Utilisation de cette politique	1744
Détails de la politique	1744
Version de la politique	1744
Document de politique JSON	1744
En savoir plus	1746
AutoScalingConsoleReadOnlyAccess	1746
Utilisation de cette politique	1746
Détails de la politique	1746
Version de la politique	1747
Document de politique JSON	1747
En savoir plus	1748
AutoScalingFullAccess	1748
Utilisation de cette politique	1748
Détails de la politique	1748
Version de la politique	1748
Document de politique JSON	1749
En savoir plus	1750
AutoScalingNotificationAccessRole	1750
Utilisation de cette politique	1750
Détails de la politique	1750
Version de la politique	1751
Document de politique JSON	1751
En savoir plus	1751
AutoScalingReadOnlyAccess	1751
Utilisation de cette politique	1752
Détails de la politique	1752
Version de la politique	1752
Document de politique JSON	1752
En savoir plus	1752

AutoScalingServiceRolePolicy	1753
Utilisation de cette politique	1753
Détails de la politique	1753
Version de la politique	1753
Document de politique JSON	1753
En savoir plus	1756
AWS-SSM-Automation-DiagnosisBucketPolicy	1757
Utilisation de cette politique	1757
Détails de la politique	1757
Version de la politique	1757
Document de politique JSON	1757
En savoir plus	1760
AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy	1760
Utilisation de cette politique	1760
Détails de la politique	1760
Version de la politique	1760
Document de politique JSON	1761
En savoir plus	1763
AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy	1763
Utilisation de cette politique	1763
Détails de la politique	1764
Version de la politique	1764
Document de politique JSON	1764
En savoir plus	1767
AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy	1767
Utilisation de cette politique	1767
Détails de la politique	1767
Version de la politique	1767
Document de politique JSON	1768
En savoir plus	1768
AWS-SSM-RemediationAutomation-AdministrationRolePolicy	1769
Utilisation de cette politique	1769
Détails de la politique	1769
Version de la politique	1769
Document de politique JSON	1769
En savoir plus	1772

AWS-SSM-RemediationAutomation-ExecutionRolePolicy	1772
Utilisation de cette politique	1772
Détails de la politique	1772
Version de la politique	1773
Document de politique JSON	1773
En savoir plus	1779
AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy	1779
Utilisation de cette politique	1779
Détails de la politique	1780
Version de la politique	1780
Document de politique JSON	1780
En savoir plus	1781
AWS_ConfigRole	1781
Utilisation de cette politique	1781
Détails de la politique	1781
Version de la politique	1781
Document de politique JSON	1782
En savoir plus	1840
AWSAccountActivityAccess	1840
Utilisation de cette politique	1840
Détails de la politique	1841
Version de la politique	1841
Document de politique JSON	1841
En savoir plus	1842
AWSAccountManagementFullAccess	1842
Utilisation de cette politique	1842
Détails de la politique	1842
Version de la politique	1842
Document de politique JSON	1843
En savoir plus	1843
AWSAccountManagementReadOnlyAccess	1843
Utilisation de cette politique	1843
Détails de la politique	1843
Version de la politique	1844
Document de politique JSON	1844
En savoir plus	1844

AWSAccountSettingsManagementRole	1844
Utilisation de cette politique	1844
Détails de la politique	1845
Version de la politique	1845
Document de politique JSON	1845
En savoir plus	1848
AWSAccountUsageReportAccess	1848
Utilisation de cette politique	1848
Détails de la politique	1848
Version de la politique	1848
Document de politique JSON	1849
En savoir plus	1849
AWSAgentlessDiscoveryService	1849
Utilisation de cette politique	1849
Détails de la politique	1850
Version de la politique	1850
Document de politique JSON	1850
En savoir plus	1852
AWSAgentRegistryServiceRolePolicy	1852
Utilisation de cette politique	1852
Détails de la politique	1852
Version de la politique	1853
Document de politique JSON	1853
En savoir plus	1855
AWSAppConfigServiceRolePolicy	1855
Utilisation de cette politique	1855
Détails de la politique	1855
Version de la politique	1856
Document de politique JSON	1856
En savoir plus	1856
AWSAppFabricFullAccess	1857
Utilisation de cette politique	1857
Détails de la politique	1857
Version de la politique	1857
Document de politique JSON	1857
En savoir plus	1859

AWSAppFabricReadOnlyAccess	1859
Utilisation de cette politique	1859
Détails de la politique	1859
Version de la politique	1859
Document de politique JSON	1859
En savoir plus	1860
AWSAppFabricServiceRolePolicy	1860
Utilisation de cette politique	1860
Détails de la politique	1860
Version de la politique	1861
Document de politique JSON	1861
En savoir plus	1862
AWSApplicationAutoscalingAppStreamFleetPolicy	1862
Utilisation de cette politique	1862
Détails de la politique	1862
Version de la politique	1863
Document de politique JSON	1863
En savoir plus	1863
AWSApplicationAutoscalingCassandraTablePolicy	1864
Utilisation de cette politique	1864
Détails de la politique	1864
Version de la politique	1864
Document de politique JSON	1864
En savoir plus	1865
AWSApplicationAutoscalingComprehendEndpointPolicy	1865
Utilisation de cette politique	1865
Détails de la politique	1865
Version de la politique	1866
Document de politique JSON	1866
En savoir plus	1866
AWSApplicationAutoScalingCustomResourcePolicy	1866
Utilisation de cette politique	1867
Détails de la politique	1867
Version de la politique	1867
Document de politique JSON	1867
En savoir plus	1868

AWSApplicationAutoscalingDynamoDBTablePolicy	1868
Utilisation de cette politique	1868
Détails de la politique	1868
Version de la politique	1868
Document de politique JSON	1868
En savoir plus	1869
AWSApplicationAutoscalingEC2SpotFleetRequestPolicy	1869
Utilisation de cette politique	1869
Détails de la politique	1869
Version de la politique	1870
Document de politique JSON	1870
En savoir plus	1870
AWSApplicationAutoscalingECSServicePolicy	1871
Utilisation de cette politique	1871
Détails de la politique	1871
Version de la politique	1871
Document de politique JSON	1871
En savoir plus	1872
AWSApplicationAutoscalingElastiCacheRGPolicy	1872
Utilisation de cette politique	1872
Détails de la politique	1872
Version de la politique	1873
Document de politique JSON	1873
En savoir plus	1874
AWSApplicationAutoscalingEMRInstanceGroupPolicy	1874
Utilisation de cette politique	1874
Détails de la politique	1874
Version de la politique	1874
Document de politique JSON	1875
En savoir plus	1875
AWSApplicationAutoscalingKafkaClusterPolicy	1875
Utilisation de cette politique	1875
Détails de la politique	1876
Version de la politique	1876
Document de politique JSON	1876
En savoir plus	1877

AWSApplicationAutoscalingLambdaConcurrencyPolicy	1877
Utilisation de cette politique	1877
Détails de la politique	1877
Version de la politique	1877
Document de politique JSON	1877
En savoir plus	1878
AWSApplicationAutoscalingNeptuneClusterPolicy	1878
Utilisation de cette politique	1878
Détails de la politique	1878
Version de la politique	1879
Document de politique JSON	1879
En savoir plus	1880
AWSApplicationAutoscalingRDSClusterPolicy	1881
Utilisation de cette politique	1881
Détails de la politique	1881
Version de la politique	1881
Document de politique JSON	1881
En savoir plus	1882
AWSApplicationAutoscalingSageMakerEndpointPolicy	1882
Utilisation de cette politique	1882
Détails de la politique	1883
Version de la politique	1883
Document de politique JSON	1883
En savoir plus	1884
AWSApplicationAutoscalingWorkSpacesPoolPolicy	1884
Utilisation de cette politique	1884
Détails de la politique	1884
Version de la politique	1885
Document de politique JSON	1885
En savoir plus	1886
AWSApplicationDiscoveryAgentAccess	1886
Utilisation de cette politique	1886
Détails de la politique	1886
Version de la politique	1887
Document de politique JSON	1887
En savoir plus	1887

AWSApplicationDiscoveryAgentlessCollectorAccess	1888
Utilisation de cette politique	1888
Détails de la politique	1888
Version de la politique	1888
Document de politique JSON	1888
En savoir plus	1889
AWSApplicationDiscoveryServiceFullAccess	1890
Utilisation de cette politique	1890
Détails de la politique	1890
Version de la politique	1890
Document de politique JSON	1890
En savoir plus	1892
AWSApplicationMigrationAgentInstallationPolicy	1892
Utilisation de cette politique	1892
Détails de la politique	1892
Version de la politique	1892
Document de politique JSON	1893
En savoir plus	1894
AWSApplicationMigrationAgentPolicy	1894
Utilisation de cette politique	1894
Détails de la politique	1894
Version de la politique	1894
Document de politique JSON	1895
En savoir plus	1895
AWSApplicationMigrationAgentPolicy_v2	1896
Utilisation de cette politique	1896
Détails de la politique	1896
Version de la politique	1896
Document de politique JSON	1896
En savoir plus	1897
AWSApplicationMigrationConversionServerPolicy	1897
Utilisation de cette politique	1898
Détails de la politique	1898
Version de la politique	1898
Document de politique JSON	1898
En savoir plus	1899

AWSApplicationMigrationEC2Access	1899
Utilisation de cette politique	1899
Détails de la politique	1899
Version de la politique	1899
Document de politique JSON	1900
En savoir plus	1908
AWSApplicationMigrationFSxProxyPolicy	1908
Utilisation de cette politique	1908
Détails de la politique	1908
Version de la politique	1908
Document de politique JSON	1909
En savoir plus	1911
AWSApplicationMigrationFSxProxyVPCPolicy	1912
Utilisation de cette politique	1912
Détails de la politique	1912
Version de la politique	1912
Document de politique JSON	1912
En savoir plus	1917
AWSApplicationMigrationFullAccess	1917
Utilisation de cette politique	1917
Détails de la politique	1917
Version de la politique	1917
Document de politique JSON	1918
En savoir plus	1926
AWSApplicationMigrationMGHAccess	1926
Utilisation de cette politique	1926
Détails de la politique	1926
Version de la politique	1927
Document de politique JSON	1927
En savoir plus	1927
AWSApplicationMigrationNetworkMigrationCustomResource	1928
Utilisation de cette politique	1928
Détails de la politique	1928
Version de la politique	1928
Document de politique JSON	1928
En savoir plus	1929

AWSApplicationMigrationNetworkMigrationMultiAccount	1929
Utilisation de cette politique	1929
Détails de la politique	1929
Version de la politique	1930
Document de politique JSON	1930
En savoir plus	1955
AWSApplicationMigrationReadOnlyAccess	1955
Utilisation de cette politique	1956
Détails de la politique	1956
Version de la politique	1956
Document de politique JSON	1956
En savoir plus	1957
AWSApplicationMigrationReplicationServerPolicy	1958
Utilisation de cette politique	1958
Détails de la politique	1958
Version de la politique	1958
Document de politique JSON	1958
En savoir plus	1960
AWSApplicationMigrationServiceEc2InstancePolicy	1960
Utilisation de cette politique	1961
Détails de la politique	1961
Version de la politique	1961
Document de politique JSON	1961
En savoir plus	1962
AWSApplicationMigrationServiceRolePolicy	1962
Utilisation de cette politique	1963
Détails de la politique	1963
Version de la politique	1963
Document de politique JSON	1963
En savoir plus	1970
AWSApplicationMigrationSSMAccess	1971
Utilisation de cette politique	1971
Détails de la politique	1971
Version de la politique	1971
Document de politique JSON	1971
En savoir plus	1973

AWSApplicationMigrationVCenterClientPolicy	1973
Utilisation de cette politique	1974
Détails de la politique	1974
Version de la politique	1974
Document de politique JSON	1974
En savoir plus	1975
AWSAppMeshEnvoyAccess	1975
Utilisation de cette politique	1975
Détails de la politique	1975
Version de la politique	1975
Document de politique JSON	1976
En savoir plus	1976
AWSAppMeshFullAccess	1976
Utilisation de cette politique	1976
Détails de la politique	1976
Version de la politique	1977
Document de politique JSON	1977
En savoir plus	1978
AWSAppMeshPreviewEnvoyAccess	1978
Utilisation de cette politique	1979
Détails de la politique	1979
Version de la politique	1979
Document de politique JSON	1979
En savoir plus	1979
AWSAppMeshPreviewServiceRolePolicy	1980
Utilisation de cette politique	1980
Détails de la politique	1980
Version de la politique	1980
Document de politique JSON	1980
En savoir plus	1981
AWSAppMeshReadOnly	1981
Utilisation de cette politique	1981
Détails de la politique	1981
Version de la politique	1982
Document de politique JSON	1982
En savoir plus	1983

AWSAppMeshServiceRolePolicy	1983
Utilisation de cette politique	1983
Détails de la politique	1983
Version de la politique	1983
Document de politique JSON	1984
En savoir plus	1984
AWSAppRunnerFullAccess	1984
Utilisation de cette politique	1985
Détails de la politique	1985
Version de la politique	1985
Document de politique JSON	1985
En savoir plus	1986
AWSAppRunnerReadOnlyAccess	1986
Utilisation de cette politique	1986
Détails de la politique	1986
Version de la politique	1987
Document de politique JSON	1987
En savoir plus	1987
AWSAppRunnerServicePolicyForECRAccess	1987
Utilisation de cette politique	1988
Détails de la politique	1988
Version de la politique	1988
Document de politique JSON	1988
En savoir plus	1989
AWSAppSyncAdministrator	1989
Utilisation de cette politique	1989
Détails de la politique	1989
Version de la politique	1989
Document de politique JSON	1990
En savoir plus	1991
AWSAppSyncInvokeFullAccess	1991
Utilisation de cette politique	1991
Détails de la politique	1991
Version de la politique	1991
Document de politique JSON	1992
En savoir plus	1992

AWSAppSyncPushToCloudWatchLogs	1992
Utilisation de cette politique	1992
Détails de la politique	1992
Version de la politique	1993
Document de politique JSON	1993
En savoir plus	1993
AWSAppSyncSchemaAuthor	1993
Utilisation de cette politique	1994
Détails de la politique	1994
Version de la politique	1994
Document de politique JSON	1994
En savoir plus	1995
AWSAppSyncServiceRolePolicy	1995
Utilisation de cette politique	1996
Détails de la politique	1996
Version de la politique	1996
Document de politique JSON	1996
En savoir plus	1997
AWSArtifactAccountSync	1997
Utilisation de cette politique	1997
Détails de la politique	1997
Version de la politique	1997
Document de politique JSON	1997
En savoir plus	1998
AWSArtifactAgreementsFullAccess	1998
Utilisation de cette politique	1998
Détails de la politique	1998
Version de la politique	1999
Document de politique JSON	1999
En savoir plus	2001
AWSArtifactAgreementsReadOnlyAccess	2001
Utilisation de cette politique	2001
Détails de la politique	2001
Version de la politique	2002
Document de politique JSON	2002
En savoir plus	2003

AWSArtifactComplianceInquiriesFullAccess	2003
Utilisation de cette politique	2003
Détails de la politique	2003
Version de la politique	2003
Document de politique JSON	2004
En savoir plus	2005
AWSArtifactComplianceInquiriesReadOnlyAccess	2005
Utilisation de cette politique	2005
Détails de la politique	2005
Version de la politique	2005
Document de politique JSON	2006
En savoir plus	2006
AWSArtifactReportsReadOnlyAccess	2006
Utilisation de cette politique	2007
Détails de la politique	2007
Version de la politique	2007
Document de politique JSON	2007
En savoir plus	2008
AWSArtifactServiceRolePolicy	2008
Utilisation de cette politique	2008
Détails de la politique	2008
Version de la politique	2008
Document de politique JSON	2009
En savoir plus	2009
AWSAuditManagerAdministratorAccess	2009
Utilisation de cette politique	2009
Détails de la politique	2009
Version de la politique	2010
Document de politique JSON	2010
En savoir plus	2014
AWSAuditManagerServiceRolePolicy	2014
Utilisation de cette politique	2014
Détails de la politique	2014
Version de la politique	2015
Document de politique JSON	2015
En savoir plus	2021

AWSAutoScalingPlansEC2AutoScalingPolicy	2022
Utilisation de cette politique	2022
Détails de la politique	2022
Version de la politique	2022
Document de politique JSON	2022
En savoir plus	2023
AWSBackupAccessPointOperatorAccess	2023
Utilisation de cette politique	2023
Détails de la politique	2023
Version de la politique	2023
Document de politique JSON	2024
En savoir plus	2025
AWSBackupAuditAccess	2025
Utilisation de cette politique	2026
Détails de la politique	2026
Version de la politique	2026
Document de politique JSON	2026
En savoir plus	2027
AWSBackupDataTransferAccess	2028
Utilisation de cette politique	2028
Détails de la politique	2028
Version de la politique	2028
Document de politique JSON	2028
En savoir plus	2029
AWSBackupFullAccess	2029
Utilisation de cette politique	2029
Détails de la politique	2029
Version de la politique	2030
Document de politique JSON	2030
En savoir plus	2042
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync	2042
Utilisation de cette politique	2042
Détails de la politique	2042
Version de la politique	2042
Document de politique JSON	2043
En savoir plus	2043

AWSBackupGuardDutyRolePolicyForScans	2043
Utilisation de cette politique	2044
Détails de la politique	2044
Version de la politique	2044
Document de politique JSON	2044
En savoir plus	2048
AWSBackupOperatorAccess	2048
Utilisation de cette politique	2048
Détails de la politique	2049
Version de la politique	2049
Document de politique JSON	2049
En savoir plus	2058
AWSBackupOrganizationAdminAccess	2058
Utilisation de cette politique	2058
Détails de la politique	2058
Version de la politique	2059
Document de politique JSON	2059
En savoir plus	2061
AWSBackupRestoreAccessForSAPHANA	2061
Utilisation de cette politique	2061
Détails de la politique	2061
Version de la politique	2061
Document de politique JSON	2062
En savoir plus	2062
AWSBackupSearchOperatorAccess	2063
Utilisation de cette politique	2063
Détails de la politique	2063
Version de la politique	2063
Document de politique JSON	2063
En savoir plus	2065
AWSBackupServiceLinkedRolePolicyForBackup	2065
Utilisation de cette politique	2065
Détails de la politique	2065
Version de la politique	2066
Document de politique JSON	2066
En savoir plus	2076

AWSBackupServiceLinkedRolePolicyForBackupTest	2076
Utilisation de cette politique	2076
Détails de la politique	2076
Version de la politique	2077
Document de politique JSON	2077
En savoir plus	2078
AWSBackupServiceRolePolicyForBackup	2078
Utilisation de cette politique	2078
Détails de la politique	2078
Version de la politique	2078
Document de politique JSON	2078
En savoir plus	2093
AWSBackupServiceRolePolicyForIndexing	2093
Utilisation de cette politique	2093
Détails de la politique	2094
Version de la politique	2094
Document de politique JSON	2094
En savoir plus	2095
AWSBackupServiceRolePolicyForItemRestores	2095
Utilisation de cette politique	2095
Détails de la politique	2096
Version de la politique	2096
Document de politique JSON	2096
En savoir plus	2098
AWSBackupServiceRolePolicyForRestores	2098
Utilisation de cette politique	2098
Détails de la politique	2098
Version de la politique	2099
Document de politique JSON	2099
En savoir plus	2113
AWSBackupServiceRolePolicyForS3Backup	2113
Utilisation de cette politique	2113
Détails de la politique	2113
Version de la politique	2113
Document de politique JSON	2114
En savoir plus	2116

AWSBackupServiceRolePolicyForS3Restore	2116
Utilisation de cette politique	2117
Détails de la politique	2117
Version de la politique	2117
Document de politique JSON	2117
En savoir plus	2118
AWSBackupServiceRolePolicyForScans	2119
Utilisation de cette politique	2119
Détails de la politique	2119
Version de la politique	2119
Document de politique JSON	2119
En savoir plus	2120
AWSBatchFullAccess	2120
Utilisation de cette politique	2121
Détails de la politique	2121
Version de la politique	2121
Document de politique JSON	2121
En savoir plus	2122
AWSBatchServiceEventTargetRole	2123
Utilisation de cette politique	2123
Détails de la politique	2123
Version de la politique	2123
Document de politique JSON	2123
En savoir plus	2124
AWSBatchServiceRole	2124
Utilisation de cette politique	2124
Détails de la politique	2124
Version de la politique	2124
Document de politique JSON	2125
En savoir plus	2128
AWSBatchServiceRolePolicyForSageMaker	2128
Utilisation de cette politique	2128
Détails de la politique	2128
Version de la politique	2129
Document de politique JSON	2129
En savoir plus	2130

AWSBCMDDataExportsServiceRolePolicy	2130
Utilisation de cette politique	2131
Détails de la politique	2131
Version de la politique	2131
Document de politique JSON	2131
En savoir plus	2132
AWSBedrockAgentCoreGatewayNetworkServiceRolePolicy	2132
Utilisation de cette politique	2132
Détails de la politique	2132
Version de la politique	2132
Document de politique JSON	2132
En savoir plus	2134
AWSBedrockAgentCoreIdentityNetworkServiceRolePolicy	2134
Utilisation de cette politique	2134
Détails de la politique	2134
Version de la politique	2135
Document de politique JSON	2135
En savoir plus	2137
AWSBedrockAgentCoreRuntimeInstancesServiceRolePolicy	2137
Utilisation de cette politique	2137
Détails de la politique	2137
Version de la politique	2137
Document de politique JSON	2137
En savoir plus	2140
AWSBillingConductorFullAccess	2140
Utilisation de cette politique	2140
Détails de la politique	2140
Version de la politique	2141
Document de politique JSON	2141
En savoir plus	2141
AWSBillingConductorReadOnlyAccess	2142
Utilisation de cette politique	2142
Détails de la politique	2142
Version de la politique	2142
Document de politique JSON	2142
En savoir plus	2143

AWSBillingConductorRolePolicy	2143
Utilisation de cette politique	2143
Détails de la politique	2144
Version de la politique	2144
Document de politique JSON	2144
En savoir plus	2145
AWSBillingReadOnlyAccess	2145
Utilisation de cette politique	2145
Détails de la politique	2145
Version de la politique	2145
Document de politique JSON	2145
En savoir plus	2148
AWSBillingServiceRolePolicy	2148
Utilisation de cette politique	2148
Détails de la politique	2148
Version de la politique	2148
Document de politique JSON	2148
En savoir plus	2149
AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM	2149
Utilisation de cette politique	2149
Détails de la politique	2149
Version de la politique	2150
Document de politique JSON	2150
En savoir plus	2151
AWSBudgetsActionsWithAWSResourceControlAccess	2151
Utilisation de cette politique	2151
Détails de la politique	2151
Version de la politique	2152
Document de politique JSON	2152
En savoir plus	2153
AWSBudgetsReadOnlyAccess	2153
Utilisation de cette politique	2153
Détails de la politique	2153
Version de la politique	2154
Document de politique JSON	2154
En savoir plus	2154

AWSBudgetsSpendLimitMemberRolePolicy	2155
Utilisation de cette politique	2155
Détails de la politique	2155
Version de la politique	2155
Document de politique JSON	2155
En savoir plus	2161
AWSBugBustFullAccess	2161
Utilisation de cette politique	2161
Détails de la politique	2161
Version de la politique	2162
Document de politique JSON	2162
En savoir plus	2163
AWSBugBustPlayerAccess	2163
Utilisation de cette politique	2163
Détails de la politique	2163
Version de la politique	2164
Document de politique JSON	2164
En savoir plus	2165
AWSBugBustServiceRolePolicy	2165
Utilisation de cette politique	2165
Détails de la politique	2165
Version de la politique	2165
Document de politique JSON	2166
En savoir plus	2166
AWSCertificateManagerFullAccess	2166
Utilisation de cette politique	2166
Détails de la politique	2167
Version de la politique	2167
Document de politique JSON	2167
En savoir plus	2168
AWSCertificateManagerPrivateCAAuditor	2168
Utilisation de cette politique	2168
Détails de la politique	2168
Version de la politique	2169
Document de politique JSON	2169
En savoir plus	2169

AWSCertificateManagerPrivateCAFullAccess	2170
Utilisation de cette politique	2170
Détails de la politique	2170
Version de la politique	2170
Document de politique JSON	2170
En savoir plus	2171
AWSCertificateManagerPrivateCAPrivilegedUser	2171
Utilisation de cette politique	2171
Détails de la politique	2171
Version de la politique	2171
Document de politique JSON	2172
En savoir plus	2173
AWSCertificateManagerPrivateCAReadOnly	2173
Utilisation de cette politique	2173
Détails de la politique	2173
Version de la politique	2174
Document de politique JSON	2174
En savoir plus	2174
AWSCertificateManagerPrivateCAUser	2175
Utilisation de cette politique	2175
Détails de la politique	2175
Version de la politique	2175
Document de politique JSON	2175
En savoir plus	2176
AWSCertificateManagerReadOnly	2177
Utilisation de cette politique	2177
Détails de la politique	2177
Version de la politique	2177
Document de politique JSON	2177
En savoir plus	2178
AWSChatbotServiceLinkedRolePolicy	2178
Utilisation de cette politique	2178
Détails de la politique	2178
Version de la politique	2179
Document de politique JSON	2179
En savoir plus	2180

AWSCleanRoomsFullAccess	2180
Utilisation de cette politique	2180
Détails de la politique	2180
Version de la politique	2180
Document de politique JSON	2180
En savoir plus	2185
AWSCleanRoomsFullAccessNoQuerying	2185
Utilisation de cette politique	2185
Détails de la politique	2185
Version de la politique	2185
Document de politique JSON	2186
En savoir plus	2190
AWSCleanRoomsMLFullAccess	2191
Utilisation de cette politique	2191
Détails de la politique	2191
Version de la politique	2191
Document de politique JSON	2191
En savoir plus	2195
AWSCleanRoomsMLReadOnlyAccess	2195
Utilisation de cette politique	2196
Détails de la politique	2196
Version de la politique	2196
Document de politique JSON	2196
En savoir plus	2197
AWSCleanRoomsReadOnlyAccess	2197
Utilisation de cette politique	2198
Détails de la politique	2198
Version de la politique	2198
Document de politique JSON	2198
En savoir plus	2199
AWSCleanRoomsServiceRolePolicy	2200
Utilisation de cette politique	2200
Détails de la politique	2200
Version de la politique	2200
Document de politique JSON	2200
En savoir plus	2201

AWSCloud9Administrator	2201
Utilisation de cette politique	2201
Détails de la politique	2201
Version de la politique	2201
Document de politique JSON	2202
En savoir plus	2203
AWSCloud9EnvironmentMember	2203
Utilisation de cette politique	2204
Détails de la politique	2204
Version de la politique	2204
Document de politique JSON	2204
En savoir plus	2206
AWSCloud9ServiceRolePolicy	2206
Utilisation de cette politique	2206
Détails de la politique	2206
Version de la politique	2206
Document de politique JSON	2207
En savoir plus	2209
AWSCloud9SSMInstanceProfile	2209
Utilisation de cette politique	2209
Détails de la politique	2210
Version de la politique	2210
Document de politique JSON	2210
En savoir plus	2210
AWSCloud9User	2211
Utilisation de cette politique	2211
Détails de la politique	2211
Version de la politique	2211
Document de politique JSON	2211
En savoir plus	2214
AWSCloudFormationFullAccess	2214
Utilisation de cette politique	2214
Détails de la politique	2214
Version de la politique	2214
Document de politique JSON	2215
En savoir plus	2215

AWSCloudFormationReadOnlyAccess	2215
Utilisation de cette politique	2215
Détails de la politique	2215
Version de la politique	2216
Document de politique JSON	2216
En savoir plus	2216
AWSCloudFrontLogger	2217
Utilisation de cette politique	2217
Détails de la politique	2217
Version de la politique	2217
Document de politique JSON	2217
En savoir plus	2218
AWSCloudFrontVPCOriginServiceRolePolicy	2218
Utilisation de cette politique	2218
Détails de la politique	2218
Version de la politique	2218
Document de politique JSON	2219
En savoir plus	2221
AWSCloudHSMFullAccess	2221
Utilisation de cette politique	2222
Détails de la politique	2222
Version de la politique	2222
Document de politique JSON	2222
En savoir plus	2222
AWSCloudHSMReadOnlyAccess	2223
Utilisation de cette politique	2223
Détails de la politique	2223
Version de la politique	2223
Document de politique JSON	2223
En savoir plus	2224
AWSCloudHSMRole	2224
Utilisation de cette politique	2224
Détails de la politique	2224
Version de la politique	2224
Document de politique JSON	2225
En savoir plus	2225

AWSCloudMapDiscoverInstanceAccess	2225
Utilisation de cette politique	2226
Détails de la politique	2226
Version de la politique	2226
Document de politique JSON	2226
En savoir plus	2227
AWSCloudMapFullAccess	2227
Utilisation de cette politique	2227
Détails de la politique	2227
Version de la politique	2227
Document de politique JSON	2227
En savoir plus	2228
AWSCloudMapReadOnlyAccess	2228
Utilisation de cette politique	2228
Détails de la politique	2229
Version de la politique	2229
Document de politique JSON	2229
En savoir plus	2229
AWSCloudMapRegisterInstanceAccess	2230
Utilisation de cette politique	2230
Détails de la politique	2230
Version de la politique	2230
Document de politique JSON	2230
En savoir plus	2231
AWSCloudShellFullAccess	2231
Utilisation de cette politique	2231
Détails de la politique	2231
Version de la politique	2232
Document de politique JSON	2232
En savoir plus	2232
AWSCloudTrail_FullAccess	2232
Utilisation de cette politique	2233
Détails de la politique	2233
Version de la politique	2233
Document de politique JSON	2233
En savoir plus	2236

AWSCloudTrail_ReadOnlyAccess	2236
Utilisation de cette politique	2236
Détails de la politique	2236
Version de la politique	2236
Document de politique JSON	2236
En savoir plus	2237
AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy	2237
Utilisation de cette politique	2237
Détails de la politique	2237
Version de la politique	2238
Document de politique JSON	2238
En savoir plus	2238
AWSCloudWatchOmniServiceRolePolicy	2238
Utilisation de cette politique	2239
Détails de la politique	2239
Version de la politique	2239
Document de politique JSON	2239
En savoir plus	2243
AWSCodeArtifactAdminAccess	2243
Utilisation de cette politique	2243
Détails de la politique	2243
Version de la politique	2243
Document de politique JSON	2244
En savoir plus	2244
AWSCodeArtifactReadOnlyAccess	2244
Utilisation de cette politique	2245
Détails de la politique	2245
Version de la politique	2245
Document de politique JSON	2245
En savoir plus	2246
AWSCodeBuildAdminAccess	2246
Utilisation de cette politique	2246
Détails de la politique	2246
Version de la politique	2246
Document de politique JSON	2247
En savoir plus	2250

AWSCodeBuildDeveloperAccess	2250
Utilisation de cette politique	2251
Détails de la politique	2251
Version de la politique	2251
Document de politique JSON	2251
En savoir plus	2254
AWSCodeBuildReadOnlyAccess	2254
Utilisation de cette politique	2254
Détails de la politique	2254
Version de la politique	2255
Document de politique JSON	2255
En savoir plus	2256
AWSCodeCommitFullAccess	2256
Utilisation de cette politique	2257
Détails de la politique	2257
Version de la politique	2257
Document de politique JSON	2257
En savoir plus	2262
AWSCodeCommitPowerUser	2262
Utilisation de cette politique	2262
Détails de la politique	2262
Version de la politique	2262
Document de politique JSON	2263
En savoir plus	2267
AWSCodeCommitReadOnly	2268
Utilisation de cette politique	2268
Détails de la politique	2268
Version de la politique	2268
Document de politique JSON	2268
En savoir plus	2271
AWSCodeDeployDeployerAccess	2271
Utilisation de cette politique	2271
Détails de la politique	2271
Version de la politique	2271
Document de politique JSON	2272
En savoir plus	2273

AWSCodeDeployFullAccess	2273
Utilisation de cette politique	2273
Détails de la politique	2274
Version de la politique	2274
Document de politique JSON	2274
En savoir plus	2276
AWSCodeDeployReadOnlyAccess	2276
Utilisation de cette politique	2276
Détails de la politique	2276
Version de la politique	2276
Document de politique JSON	2276
En savoir plus	2277
AWSCodeDeployRole	2278
Utilisation de cette politique	2278
Détails de la politique	2278
Version de la politique	2278
Document de politique JSON	2278
En savoir plus	2280
AWSCodeDeployRoleForCloudFormation	2280
Utilisation de cette politique	2280
Détails de la politique	2280
Version de la politique	2280
Document de politique JSON	2281
En savoir plus	2281
AWSCodeDeployRoleForECS	2281
Utilisation de cette politique	2281
Détails de la politique	2281
Version de la politique	2282
Document de politique JSON	2282
En savoir plus	2283
AWSCodeDeployRoleForECSLimited	2283
Utilisation de cette politique	2283
Détails de la politique	2283
Version de la politique	2284
Document de politique JSON	2284
En savoir plus	2285

AWSCodeDeployRoleForLambda	2286
Utilisation de cette politique	2286
Détails de la politique	2286
Version de la politique	2286
Document de politique JSON	2286
En savoir plus	2287
AWSCodeDeployRoleForLambdaLimited	2288
Utilisation de cette politique	2288
Détails de la politique	2288
Version de la politique	2288
Document de politique JSON	2288
En savoir plus	2289
AWSCodePipeline_FullAccess	2290
Utilisation de cette politique	2290
Détails de la politique	2290
Version de la politique	2290
Document de politique JSON	2290
En savoir plus	2294
AWSCodePipeline_ReadOnlyAccess	2294
Utilisation de cette politique	2294
Détails de la politique	2294
Version de la politique	2295
Document de politique JSON	2295
En savoir plus	2296
AWSCodePipelineApproverAccess	2296
Utilisation de cette politique	2296
Détails de la politique	2296
Version de la politique	2297
Document de politique JSON	2297
En savoir plus	2297
AWSCodePipelineCustomActionAccess	2298
Utilisation de cette politique	2298
Détails de la politique	2298
Version de la politique	2298
Document de politique JSON	2298
En savoir plus	2299

AWSCodeStarFullAccess	2299
Utilisation de cette politique	2299
Détails de la politique	2299
Version de la politique	2299
Document de politique JSON	2300
En savoir plus	2300
AWSCodeStarNotificationsServiceRolePolicy	2301
Utilisation de cette politique	2301
Détails de la politique	2301
Version de la politique	2301
Document de politique JSON	2301
En savoir plus	2303
AWSCodeStarServiceRole	2303
Utilisation de cette politique	2303
Détails de la politique	2303
Version de la politique	2303
Document de politique JSON	2303
En savoir plus	2309
AWSCompromisedKeyQuarantine	2309
Utilisation de cette politique	2309
Détails de la politique	2309
Version de la politique	2309
Document de politique JSON	2310
En savoir plus	2311
AWSCompromisedKeyQuarantineV2	2311
Utilisation de cette politique	2311
Détails de la politique	2311
Version de la politique	2311
Document de politique JSON	2312
En savoir plus	2314
AWSCompromisedKeyQuarantineV3	2314
Utilisation de cette politique	2315
Détails de la politique	2315
Version de la politique	2315
Document de politique JSON	2315
En savoir plus	2318

AWSServiceCatalogMultiAccountSetupPolicy	2318
Utilisation de cette politique	2318
Détails de la politique	2318
Version de la politique	2319
Document de politique JSON	2319
En savoir plus	2321
AWSServiceCatalogRemediationServiceRolePolicy	2321
Utilisation de cette politique	2321
Détails de la politique	2321
Version de la politique	2321
Document de politique JSON	2322
En savoir plus	2322
AWSServiceCatalogRoleForOrganizations	2322
Utilisation de cette politique	2323
Détails de la politique	2323
Version de la politique	2323
Document de politique JSON	2323
En savoir plus	2324
AWSServiceCatalogRulesExecutionRole	2324
Utilisation de cette politique	2324
Détails de la politique	2324
Version de la politique	2324
Document de politique JSON	2325
En savoir plus	2325
AWSServiceCatalogServiceRolePolicy	2325
Utilisation de cette politique	2326
Détails de la politique	2326
Version de la politique	2326
Document de politique JSON	2326
En savoir plus	2385
AWSServiceCatalogThirdPartyServiceRolePolicy	2386
Utilisation de cette politique	2386
Détails de la politique	2386
Version de la politique	2386
Document de politique JSON	2386
En savoir plus	2387

AWSCfgUserAccess	2388
Utilisation de cette politique	2388
Détails de la politique	2388
Version de la politique	2388
Document de politique JSON	2388
En savoir plus	2389
AWSConnector	2389
Utilisation de cette politique	2389
Détails de la politique	2389
Version de la politique	2390
Document de politique JSON	2390
En savoir plus	2392
AWSCtrlTowerAccountServiceRolePolicy	2392
Utilisation de cette politique	2392
Détails de la politique	2392
Version de la politique	2392
Document de politique JSON	2393
En savoir plus	2398
AWSCtrlTowerCloudTrailRolePolicy	2398
Utilisation de cette politique	2398
Détails de la politique	2398
Version de la politique	2399
Document de politique JSON	2399
En savoir plus	2399
AWSCtrlTowerIdentityCenterManagementPolicy	2399
Utilisation de cette politique	2400
Détails de la politique	2400
Version de la politique	2400
Document de politique JSON	2400
En savoir plus	2401
AWSCtrlTowerServiceRolePolicy	2401
Utilisation de cette politique	2402
Détails de la politique	2402
Version de la politique	2402
Document de politique JSON	2402
En savoir plus	2408

AWSCostAndUsageReportAutomationPolicy	2408
Utilisation de cette politique	2408
Détails de la politique	2408
Version de la politique	2408
Document de politique JSON	2409
En savoir plus	2410
AWSDataExchangeDataGrantOwnerFullAccess	2410
Utilisation de cette politique	2410
Détails de la politique	2410
Version de la politique	2410
Document de politique JSON	2411
En savoir plus	2412
AWSDataExchangeDataGrantReceiverFullAccess	2412
Utilisation de cette politique	2412
Détails de la politique	2413
Version de la politique	2413
Document de politique JSON	2413
En savoir plus	2414
AWSDataExchangeFullAccess	2415
Utilisation de cette politique	2415
Détails de la politique	2415
Version de la politique	2415
Document de politique JSON	2415
En savoir plus	2419
AWSDataExchangeProviderFullAccess	2419
Utilisation de cette politique	2419
Détails de la politique	2419
Version de la politique	2420
Document de politique JSON	2420
En savoir plus	2424
AWSDataExchangeReadOnly	2424
Utilisation de cette politique	2424
Détails de la politique	2424
Version de la politique	2424
Document de politique JSON	2424
En savoir plus	2426

AWSDDataExchangeServiceRolePolicyForLicenseManagement	2426
Utilisation de cette politique	2426
Détails de la politique	2426
Version de la politique	2426
Document de politique JSON	2427
En savoir plus	2427
AWSDDataExchangeServiceRolePolicyForOrganizationDiscovery	2427
Utilisation de cette politique	2427
Détails de la politique	2428
Version de la politique	2428
Document de politique JSON	2428
En savoir plus	2428
AWSDDataExchangeSubscriberFullAccess	2429
Utilisation de cette politique	2429
Détails de la politique	2429
Version de la politique	2429
Document de politique JSON	2429
En savoir plus	2432
AWSDDataLifecycleManagerServiceRole	2432
Utilisation de cette politique	2432
Détails de la politique	2432
Version de la politique	2432
Document de politique JSON	2433
En savoir plus	2434
AWSDDataLifecycleManagerServiceRoleForAMIManagement	2434
Utilisation de cette politique	2434
Détails de la politique	2434
Version de la politique	2434
Document de politique JSON	2435
En savoir plus	2436
AWSDDataLifecycleManagerSSMFullAccess	2436
Utilisation de cette politique	2436
Détails de la politique	2436
Version de la politique	2437
Document de politique JSON	2437
En savoir plus	2438

AWSDatapipeline_FullAccess	2438
Utilisation de cette politique	2439
Détails de la politique	2439
Version de la politique	2439
Document de politique JSON	2439
En savoir plus	2440
AWSDatapipeline_PowerUser	2440
Utilisation de cette politique	2440
Détails de la politique	2440
Version de la politique	2441
Document de politique JSON	2441
En savoir plus	2442
AWSDatapipeline_DiscoveryServiceRolePolicy	2442
Utilisation de cette politique	2442
Détails de la politique	2442
Version de la politique	2442
Document de politique JSON	2443
En savoir plus	2444
AWSDatapipeline_FullAccess	2444
Utilisation de cette politique	2444
Détails de la politique	2444
Version de la politique	2444
Document de politique JSON	2444
En savoir plus	2447
AWSDatapipeline_ReadOnlyAccess	2447
Utilisation de cette politique	2447
Détails de la politique	2447
Version de la politique	2448
Document de politique JSON	2448
En savoir plus	2448
AWSDatapipeline_ServiceRolePolicy	2449
Utilisation de cette politique	2449
Détails de la politique	2449
Version de la politique	2449
Document de politique JSON	2449
En savoir plus	2450

AWSDeadlineCloud-FleetWorker	2451
Utilisation de cette politique	2451
Détails de la politique	2451
Version de la politique	2451
Document de politique JSON	2451
En savoir plus	2452
AWSDeadlineCloud-UserAccessFarms	2452
Utilisation de cette politique	2452
Détails de la politique	2452
Version de la politique	2453
Document de politique JSON	2453
En savoir plus	2459
AWSDeadlineCloud-UserAccessFleets	2459
Utilisation de cette politique	2459
Détails de la politique	2459
Version de la politique	2460
Document de politique JSON	2460
En savoir plus	2463
AWSDeadlineCloud-UserAccessJobs	2464
Utilisation de cette politique	2464
Détails de la politique	2464
Version de la politique	2464
Document de politique JSON	2464
En savoir plus	2468
AWSDeadlineCloud-UserAccessQueues	2468
Utilisation de cette politique	2469
Détails de la politique	2469
Version de la politique	2469
Document de politique JSON	2469
En savoir plus	2474
AWSDeadlineCloud-WorkerHost	2474
Utilisation de cette politique	2474
Détails de la politique	2474
Version de la politique	2474
Document de politique JSON	2475
En savoir plus	2476

AWSDeepLensLambdaFunctionAccessPolicy	2476
Utilisation de cette politique	2476
Détails de la politique	2476
Version de la politique	2477
Document de politique JSON	2477
En savoir plus	2478
AWSDeepLensServiceRolePolicy	2478
Utilisation de cette politique	2478
Détails de la politique	2478
Version de la politique	2479
Document de politique JSON	2479
En savoir plus	2486
AWSDeepRacerAccountAdminAccess	2486
Utilisation de cette politique	2486
Détails de la politique	2486
Version de la politique	2487
Document de politique JSON	2487
En savoir plus	2487
AWSDeepRacerCloudFormationAccessPolicy	2488
Utilisation de cette politique	2488
Détails de la politique	2488
Version de la politique	2488
Document de politique JSON	2488
En savoir plus	2491
AWSDeepRacerDefaultMultiUserAccess	2491
Utilisation de cette politique	2492
Détails de la politique	2492
Version de la politique	2492
Document de politique JSON	2492
En savoir plus	2494
AWSDeepRacerFullAccess	2494
Utilisation de cette politique	2494
Détails de la politique	2494
Version de la politique	2494
Document de politique JSON	2494
En savoir plus	2495

AWSDeepRacerRoboMakerAccessPolicy	2496
Utilisation de cette politique	2496
Détails de la politique	2496
Version de la politique	2496
Document de politique JSON	2496
En savoir plus	2498
AWSDeepRacerServiceRolePolicy	2498
Utilisation de cette politique	2499
Détails de la politique	2499
Version de la politique	2499
Document de politique JSON	2499
En savoir plus	2502
AWSDenyAll	2502
Utilisation de cette politique	2502
Détails de la politique	2503
Version de la politique	2503
Document de politique JSON	2503
En savoir plus	2503
AWSDeviceFarmFullAccess	2504
Utilisation de cette politique	2504
Détails de la politique	2504
Version de la politique	2504
Document de politique JSON	2504
En savoir plus	2505
AWSDeviceFarmServiceRolePolicy	2505
Utilisation de cette politique	2505
Détails de la politique	2505
Version de la politique	2505
Document de politique JSON	2506
En savoir plus	2508
AWSDeviceFarmTestGridServiceRolePolicy	2508
Utilisation de cette politique	2508
Détails de la politique	2508
Version de la politique	2508
Document de politique JSON	2508
En savoir plus	2511

AWSDirectConnectFullAccess	2511
Utilisation de cette politique	2511
Détails de la politique	2511
Version de la politique	2511
Document de politique JSON	2511
En savoir plus	2512
AWSDirectConnectReadOnlyAccess	2512
Utilisation de cette politique	2512
Détails de la politique	2512
Version de la politique	2512
Document de politique JSON	2513
En savoir plus	2513
AWSDirectConnectServiceRolePolicy	2513
Utilisation de cette politique	2514
Détails de la politique	2514
Version de la politique	2514
Document de politique JSON	2514
En savoir plus	2515
AWSDirectoryServiceDataFullAccess	2515
Utilisation de cette politique	2515
Détails de la politique	2515
Version de la politique	2515
Document de politique JSON	2515
En savoir plus	2516
AWSDirectoryServiceDataReadOnlyAccess	2516
Utilisation de cette politique	2517
Détails de la politique	2517
Version de la politique	2517
Document de politique JSON	2517
En savoir plus	2518
AWSDirectoryServiceFullAccess	2518
Utilisation de cette politique	2518
Détails de la politique	2518
Version de la politique	2518
Document de politique JSON	2519
En savoir plus	2520

AWSDirectoryServiceReadOnlyAccess	2521
Utilisation de cette politique	2521
Détails de la politique	2521
Version de la politique	2521
Document de politique JSON	2521
En savoir plus	2522
AWSDirectoryServiceServiceRolePolicy	2522
Utilisation de cette politique	2522
Détails de la politique	2522
Version de la politique	2523
Document de politique JSON	2523
En savoir plus	2524
AWSDiscoveryContinuousExportFirehosePolicy	2524
Utilisation de cette politique	2524
Détails de la politique	2524
Version de la politique	2525
Document de politique JSON	2525
En savoir plus	2526
AWSDMSFleetAdvisorServiceRolePolicy	2526
Utilisation de cette politique	2526
Détails de la politique	2526
Version de la politique	2526
Document de politique JSON	2527
En savoir plus	2527
AWSDMSServerlessServiceRolePolicy	2527
Utilisation de cette politique	2527
Détails de la politique	2527
Version de la politique	2528
Document de politique JSON	2528
En savoir plus	2531
AWSEC2CapacityManagerServiceRolePolicy	2531
Utilisation de cette politique	2531
Détails de la politique	2531
Version de la politique	2531
Document de politique JSON	2531
En savoir plus	2532

AWSEC2CapacityReservationFleetRolePolicy	2532
Utilisation de cette politique	2533
Détails de la politique	2533
Version de la politique	2533
Document de politique JSON	2533
En savoir plus	2534
AWSEC2FleetServiceRolePolicy	2534
Utilisation de cette politique	2535
Détails de la politique	2535
Version de la politique	2535
Document de politique JSON	2535
En savoir plus	2537
AWSEC2SpotFleetServiceRolePolicy	2537
Utilisation de cette politique	2537
Détails de la politique	2538
Version de la politique	2538
Document de politique JSON	2538
En savoir plus	2540
AWSEC2SpotServiceRolePolicy	2540
Utilisation de cette politique	2540
Détails de la politique	2540
Version de la politique	2540
Document de politique JSON	2541
En savoir plus	2542
AWSEC2SqlHaInstancePolicy	2542
Utilisation de cette politique	2542
Détails de la politique	2543
Version de la politique	2543
Document de politique JSON	2543
En savoir plus	2544
AWSEC2SqlHaServiceRolePolicy	2544
Utilisation de cette politique	2545
Détails de la politique	2545
Version de la politique	2545
Document de politique JSON	2545
En savoir plus	2547

AWSEC2VssRestorePolicy	2547
Utilisation de cette politique	2547
Détails de la politique	2547
Version de la politique	2548
Document de politique JSON	2548
En savoir plus	2550
AWSEC2VssSnapshotPolicy	2550
Utilisation de cette politique	2551
Détails de la politique	2551
Version de la politique	2551
Document de politique JSON	2551
En savoir plus	2554
AWSECRPullThroughCache_ServiceRolePolicy	2555
Utilisation de cette politique	2555
Détails de la politique	2555
Version de la politique	2555
Document de politique JSON	2555
En savoir plus	2556
AWSElasticBeanstalkCustomPlatformforEC2Role	2556
Utilisation de cette politique	2557
Détails de la politique	2557
Version de la politique	2557
Document de politique JSON	2557
En savoir plus	2559
AWSElasticBeanstalkEKSIImageBuild	2559
Utilisation de cette politique	2559
Détails de la politique	2559
Version de la politique	2559
Document de politique JSON	2560
En savoir plus	2562
AWSElasticBeanstalkEKSObservability	2562
Utilisation de cette politique	2562
Détails de la politique	2562
Version de la politique	2562
Document de politique JSON	2563
En savoir plus	2564

AWSElasticBeanstalkEKSTagging	2564
Utilisation de cette politique	2565
Détails de la politique	2565
Version de la politique	2565
Document de politique JSON	2565
En savoir plus	2568
AWSElasticBeanstalkEnhancedHealth	2568
Utilisation de cette politique	2568
Détails de la politique	2568
Version de la politique	2568
Document de politique JSON	2568
En savoir plus	2569
AWSElasticBeanstalkMaintenance	2570
Utilisation de cette politique	2570
Détails de la politique	2570
Version de la politique	2570
Document de politique JSON	2570
En savoir plus	2571
AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy	2571
Utilisation de cette politique	2572
Détails de la politique	2572
Version de la politique	2572
Document de politique JSON	2572
En savoir plus	2579
AWSElasticBeanstalkManagedUpdatesServiceRolePolicy	2579
Utilisation de cette politique	2579
Détails de la politique	2580
Version de la politique	2580
Document de politique JSON	2580
En savoir plus	2586
AWSElasticBeanstalkMulticontainerDocker	2586
Utilisation de cette politique	2586
Détails de la politique	2586
Version de la politique	2586
Document de politique JSON	2586
En savoir plus	2588

AWSElasticBeanstalkReadOnly	2589
Utilisation de cette politique	2589
Détails de la politique	2589
Version de la politique	2589
Document de politique JSON	2589
En savoir plus	2592
AWSElasticBeanstalkRoleCore	2592
Utilisation de cette politique	2592
Détails de la politique	2592
Version de la politique	2592
Document de politique JSON	2593
En savoir plus	2597
AWSElasticBeanstalkRoleCWL	2598
Utilisation de cette politique	2598
Détails de la politique	2598
Version de la politique	2598
Document de politique JSON	2598
En savoir plus	2599
AWSElasticBeanstalkRoleECS	2599
Utilisation de cette politique	2599
Détails de la politique	2599
Version de la politique	2599
Document de politique JSON	2600
En savoir plus	2601
AWSElasticBeanstalkRoleRDS	2601
Utilisation de cette politique	2601
Détails de la politique	2601
Version de la politique	2601
Document de politique JSON	2601
En savoir plus	2602
AWSElasticBeanstalkRoleSNS	2602
Utilisation de cette politique	2602
Détails de la politique	2603
Version de la politique	2603
Document de politique JSON	2603
En savoir plus	2604

AWSElasticBeanstalkRoleWorkerTier	2604
Utilisation de cette politique	2604
Détails de la politique	2604
Version de la politique	2604
Document de politique JSON	2605
En savoir plus	2605
AWSElasticBeanstalkService	2606
Utilisation de cette politique	2606
Détails de la politique	2606
Version de la politique	2606
Document de politique JSON	2606
En savoir plus	2611
AWSElasticBeanstalkServiceRolePolicy	2611
Utilisation de cette politique	2611
Détails de la politique	2611
Version de la politique	2611
Document de politique JSON	2612
En savoir plus	2625
AWSElasticBeanstalkWebTier	2625
Utilisation de cette politique	2626
Détails de la politique	2626
Version de la politique	2626
Document de politique JSON	2626
En savoir plus	2628
AWSElasticBeanstalkWorkerTier	2629
Utilisation de cette politique	2629
Détails de la politique	2629
Version de la politique	2629
Document de politique JSON	2629
En savoir plus	2632
AWSElasticDisasterRecoveryAgentInstallationPolicy	2633
Utilisation de cette politique	2633
Détails de la politique	2633
Version de la politique	2633
Document de politique JSON	2633
En savoir plus	2635

AWSElasticDisasterRecoveryAgentPolicy	2635
Utilisation de cette politique	2635
Détails de la politique	2635
Version de la politique	2636
Document de politique JSON	2636
En savoir plus	2637
AWSElasticDisasterRecoveryConsoleFullAccess	2637
Utilisation de cette politique	2637
Détails de la politique	2637
Version de la politique	2637
Document de politique JSON	2638
En savoir plus	2648
AWSElasticDisasterRecoveryConsoleFullAccess_v2	2648
Utilisation de cette politique	2648
Détails de la politique	2648
Version de la politique	2648
Document de politique JSON	2649
En savoir plus	2664
AWSElasticDisasterRecoveryConversionServerPolicy	2664
Utilisation de cette politique	2665
Détails de la politique	2665
Version de la politique	2665
Document de politique JSON	2665
En savoir plus	2666
AWSElasticDisasterRecoveryCrossAccountReplicationPolicy	2666
Utilisation de cette politique	2666
Détails de la politique	2666
Version de la politique	2667
Document de politique JSON	2667
En savoir plus	2668
AWSElasticDisasterRecoveryEc2InstancePolicy	2668
Utilisation de cette politique	2668
Détails de la politique	2668
Version de la politique	2668
Document de politique JSON	2669
En savoir plus	2671

AWSElasticDisasterRecoveryFailbackInstallationPolicy	2671
Utilisation de cette politique	2671
Détails de la politique	2671
Version de la politique	2671
Document de politique JSON	2672
En savoir plus	2672
AWSElasticDisasterRecoveryFailbackPolicy	2673
Utilisation de cette politique	2673
Détails de la politique	2673
Version de la politique	2673
Document de politique JSON	2673
En savoir plus	2675
AWSElasticDisasterRecoveryLaunchActionsPolicy	2675
Utilisation de cette politique	2675
Détails de la politique	2675
Version de la politique	2675
Document de politique JSON	2676
En savoir plus	2682
AWSElasticDisasterRecoveryNetworkReplicationPolicy	2682
Utilisation de cette politique	2682
Détails de la politique	2682
Version de la politique	2682
Document de politique JSON	2683
En savoir plus	2683
AWSElasticDisasterRecoveryReadOnlyAccess	2683
Utilisation de cette politique	2684
Détails de la politique	2684
Version de la politique	2684
Document de politique JSON	2684
En savoir plus	2687
AWSElasticDisasterRecoveryRecoveryInstancePolicy	2687
Utilisation de cette politique	2687
Détails de la politique	2687
Version de la politique	2687
Document de politique JSON	2688
En savoir plus	2690

AWSElasticDisasterRecoveryReplicationServerPolicy	2690
Utilisation de cette politique	2691
Détails de la politique	2691
Version de la politique	2691
Document de politique JSON	2691
En savoir plus	2693
AWSElasticDisasterRecoveryServiceRolePolicy	2694
Utilisation de cette politique	2694
Détails de la politique	2694
Version de la politique	2694
Document de politique JSON	2694
En savoir plus	2704
AWSElasticDisasterRecoveryStagingAccountPolicy	2704
Utilisation de cette politique	2705
Détails de la politique	2705
Version de la politique	2705
Document de politique JSON	2705
En savoir plus	2706
AWSElasticDisasterRecoveryStagingAccountPolicy_v2	2706
Utilisation de cette politique	2706
Détails de la politique	2707
Version de la politique	2707
Document de politique JSON	2707
En savoir plus	2708
AWSElasticLoadBalancingClassicServiceRolePolicy	2709
Utilisation de cette politique	2709
Détails de la politique	2709
Version de la politique	2709
Document de politique JSON	2709
En savoir plus	2710
AWSElasticLoadBalancingServiceRolePolicy	2710
Utilisation de cette politique	2710
Détails de la politique	2711
Version de la politique	2711
Document de politique JSON	2711
En savoir plus	2712

AWSElementalMediaConnectCreateBridge	2712
Utilisation de cette politique	2713
Détails de la politique	2713
Version de la politique	2713
Document de politique JSON	2713
En savoir plus	2714
AWSElementalMediaConnectCreateFlow	2714
Utilisation de cette politique	2714
Détails de la politique	2714
Version de la politique	2714
Document de politique JSON	2715
En savoir plus	2715
AWSElementalMediaConnectDeleteBridge	2716
Utilisation de cette politique	2716
Détails de la politique	2716
Version de la politique	2716
Document de politique JSON	2716
En savoir plus	2717
AWSElementalMediaConnectDeleteFlow	2717
Utilisation de cette politique	2717
Détails de la politique	2717
Version de la politique	2718
Document de politique JSON	2718
En savoir plus	2718
AWSElementalMediaConnectFullAccess	2719
Utilisation de cette politique	2719
Détails de la politique	2719
Version de la politique	2719
Document de politique JSON	2719
En savoir plus	2720
AWSElementalMediaConnectReadOnlyAccess	2720
Utilisation de cette politique	2720
Détails de la politique	2720
Version de la politique	2720
Document de politique JSON	2721
En savoir plus	2721

AWSElementalMediaConvertFullAccess	2722
Utilisation de cette politique	2722
Détails de la politique	2722
Version de la politique	2722
Document de politique JSON	2722
En savoir plus	2723
AWSElementalMediaConvertReadOnly	2723
Utilisation de cette politique	2723
Détails de la politique	2723
Version de la politique	2724
Document de politique JSON	2724
En savoir plus	2724
AWSElementalMediaLiveFullAccess	2725
Utilisation de cette politique	2725
Détails de la politique	2725
Version de la politique	2725
Document de politique JSON	2725
En savoir plus	2725
AWSElementalMediaLiveReadOnly	2726
Utilisation de cette politique	2726
Détails de la politique	2726
Version de la politique	2726
Document de politique JSON	2726
En savoir plus	2727
AWSElementalMediaPackageFullAccess	2727
Utilisation de cette politique	2727
Détails de la politique	2727
Version de la politique	2727
Document de politique JSON	2728
En savoir plus	2728
AWSElementalMediaPackageReadOnly	2728
Utilisation de cette politique	2728
Détails de la politique	2728
Version de la politique	2729
Document de politique JSON	2729
En savoir plus	2729

AWSElementalMediaPackageV2FullAccess	2729
Utilisation de cette politique	2729
Détails de la politique	2730
Version de la politique	2730
Document de politique JSON	2730
En savoir plus	2730
AWSElementalMediaPackageV2ReadOnly	2730
Utilisation de cette politique	2731
Détails de la politique	2731
Version de la politique	2731
Document de politique JSON	2731
En savoir plus	2731
AWSElementalMediaStoreFullAccess	2732
Utilisation de cette politique	2732
Détails de la politique	2732
Version de la politique	2732
Document de politique JSON	2732
En savoir plus	2733
AWSElementalMediaStoreReadOnly	2733
Utilisation de cette politique	2733
Détails de la politique	2733
Version de la politique	2733
Document de politique JSON	2734
En savoir plus	2734
AWSElementalMediaTailorFullAccess	2734
Utilisation de cette politique	2735
Détails de la politique	2735
Version de la politique	2735
Document de politique JSON	2735
En savoir plus	2735
AWSElementalMediaTailorReadOnly	2736
Utilisation de cette politique	2736
Détails de la politique	2736
Version de la politique	2736
Document de politique JSON	2736
En savoir plus	2737

AWSEnhancedClassicNetworkingMangementPolicy	2737
Utilisation de cette politique	2737
Détails de la politique	2737
Version de la politique	2737
Document de politique JSON	2738
En savoir plus	2738
AWSEntityResolutionConsoleFullAccess	2738
Utilisation de cette politique	2738
Détails de la politique	2738
Version de la politique	2739
Document de politique JSON	2739
En savoir plus	2742
AWSEntityResolutionConsoleReadOnlyAccess	2742
Utilisation de cette politique	2742
Détails de la politique	2742
Version de la politique	2743
Document de politique JSON	2743
En savoir plus	2743
AWSFaultInjectionSimulatorEC2Access	2743
Utilisation de cette politique	2744
Détails de la politique	2744
Version de la politique	2744
Document de politique JSON	2744
En savoir plus	2746
AWSFaultInjectionSimulatorECSAccess	2746
Utilisation de cette politique	2746
Détails de la politique	2746
Version de la politique	2746
Document de politique JSON	2747
En savoir plus	2749
AWSFaultInjectionSimulatorEKSAccess	2749
Utilisation de cette politique	2749
Détails de la politique	2749
Version de la politique	2750
Document de politique JSON	2750
En savoir plus	2751

AWSFaultInjectionSimulatorNetworkAccess	2751
Utilisation de cette politique	2751
Détails de la politique	2751
Version de la politique	2752
Document de politique JSON	2752
En savoir plus	2759
AWSFaultInjectionSimulatorRDSAccess	2759
Utilisation de cette politique	2759
Détails de la politique	2759
Version de la politique	2759
Document de politique JSON	2760
En savoir plus	2761
AWSFaultInjectionSimulatorSSMAccess	2761
Utilisation de cette politique	2761
Détails de la politique	2761
Version de la politique	2761
Document de politique JSON	2762
En savoir plus	2763
AWSFinSpaceServiceRolePolicy	2763
Utilisation de cette politique	2763
Détails de la politique	2763
Version de la politique	2764
Document de politique JSON	2764
En savoir plus	2764
AWSFMAdminFullAccess	2764
Utilisation de cette politique	2765
Détails de la politique	2765
Version de la politique	2765
Document de politique JSON	2765
En savoir plus	2767
AWSFMAdminReadOnlyAccess	2767
Utilisation de cette politique	2767
Détails de la politique	2767
Version de la politique	2768
Document de politique JSON	2768
En savoir plus	2769

AWSFMMemberReadOnlyAccess	2769
Utilisation de cette politique	2770
Détails de la politique	2770
Version de la politique	2770
Document de politique JSON	2770
En savoir plus	2771
AWSForWordPressPluginPolicy	2771
Utilisation de cette politique	2771
Détails de la politique	2771
Version de la politique	2771
Document de politique JSON	2771
En savoir plus	2774
AWSGitSyncServiceRolePolicy	2774
Utilisation de cette politique	2774
Détails de la politique	2774
Version de la politique	2775
Document de politique JSON	2775
En savoir plus	2775
AWSGlobalAcceleratorSLRPolicy	2776
Utilisation de cette politique	2776
Détails de la politique	2776
Version de la politique	2776
Document de politique JSON	2776
En savoir plus	2778
AWSGlueConsoleFullAccess	2778
Utilisation de cette politique	2778
Détails de la politique	2778
Version de la politique	2778
Document de politique JSON	2779
En savoir plus	2783
AWSGlueConsoleSageMakerNotebookFullAccess	2783
Utilisation de cette politique	2784
Détails de la politique	2784
Version de la politique	2784
Document de politique JSON	2784
En savoir plus	2790

AwsGlueDataBrewFullAccessPolicy	2790
Utilisation de cette politique	2790
Détails de la politique	2790
Version de la politique	2790
Document de politique JSON	2791
En savoir plus	2796
AWSGlueDataBrewServiceRole	2796
Utilisation de cette politique	2796
Détails de la politique	2796
Version de la politique	2796
Document de politique JSON	2797
En savoir plus	2799
AWSGlueSchemaRegistryFullAccess	2800
Utilisation de cette politique	2800
Détails de la politique	2800
Version de la politique	2800
Document de politique JSON	2800
En savoir plus	2801
AWSGlueSchemaRegistryReadOnlyAccess	2802
Utilisation de cette politique	2802
Détails de la politique	2802
Version de la politique	2802
Document de politique JSON	2802
En savoir plus	2803
AWSGlueServiceNotebookRole	2803
Utilisation de cette politique	2803
Détails de la politique	2803
Version de la politique	2804
Document de politique JSON	2804
En savoir plus	2806
AWSGlueServiceRole	2806
Utilisation de cette politique	2806
Détails de la politique	2807
Version de la politique	2807
Document de politique JSON	2807
En savoir plus	2809

AwsGlueSessionUserRestrictedNotebookPolicy	2809
Utilisation de cette politique	2810
Détails de la politique	2810
Version de la politique	2810
Document de politique JSON	2810
En savoir plus	2813
AwsGlueSessionUserRestrictedNotebookServiceRole	2813
Utilisation de cette politique	2813
Détails de la politique	2813
Version de la politique	2814
Document de politique JSON	2814
En savoir plus	2818
AwsGlueSessionUserRestrictedPolicy	2818
Utilisation de cette politique	2818
Détails de la politique	2818
Version de la politique	2819
Document de politique JSON	2819
En savoir plus	2822
AwsGlueSessionUserRestrictedServiceRole	2822
Utilisation de cette politique	2822
Détails de la politique	2822
Version de la politique	2822
Document de politique JSON	2823
En savoir plus	2827
AWSGrafanaAccountAdministrator	2827
Utilisation de cette politique	2827
Détails de la politique	2827
Version de la politique	2828
Document de politique JSON	2828
En savoir plus	2829
AWSGrafanaConsoleReadOnlyAccess	2829
Utilisation de cette politique	2829
Détails de la politique	2829
Version de la politique	2829
Document de politique JSON	2830
En savoir plus	2830

AWSGrafanaWorkspacePermissionManagement	2830
Utilisation de cette politique	2830
Détails de la politique	2830
Version de la politique	2831
Document de politique JSON	2831
En savoir plus	2832
AWSGrafanaWorkspacePermissionManagementV2	2832
Utilisation de cette politique	2832
Détails de la politique	2832
Version de la politique	2832
Document de politique JSON	2833
En savoir plus	2834
AWSGreengrassFullAccess	2834
Utilisation de cette politique	2834
Détails de la politique	2834
Version de la politique	2834
Document de politique JSON	2834
En savoir plus	2835
AWSGreengrassReadOnlyAccess	2835
Utilisation de cette politique	2835
Détails de la politique	2835
Version de la politique	2836
Document de politique JSON	2836
En savoir plus	2836
AWSGreengrassResourceAccessRolePolicy	2836
Utilisation de cette politique	2837
Détails de la politique	2837
Version de la politique	2837
Document de politique JSON	2837
En savoir plus	2839
AWSGroundStationAgentInstancePolicy	2840
Utilisation de cette politique	2840
Détails de la politique	2840
Version de la politique	2840
Document de politique JSON	2840
En savoir plus	2841

AWSHealth_EventProcessorServiceRolePolicy	2841
Utilisation de cette politique	2841
Détails de la politique	2841
Version de la politique	2841
Document de politique JSON	2842
En savoir plus	2842
AWSHealthFullAccess	2843
Utilisation de cette politique	2843
Détails de la politique	2843
Version de la politique	2843
Document de politique JSON	2843
En savoir plus	2844
AWSHealthImagingFullAccess	2844
Utilisation de cette politique	2845
Détails de la politique	2845
Version de la politique	2845
Document de politique JSON	2845
En savoir plus	2846
AWSHealthImagingReadOnlyAccess	2846
Utilisation de cette politique	2846
Détails de la politique	2846
Version de la politique	2846
Document de politique JSON	2847
En savoir plus	2847
AWSHealthImagingServiceRolePolicy	2847
Utilisation de cette politique	2848
Détails de la politique	2848
Version de la politique	2848
Document de politique JSON	2848
En savoir plus	2849
AWSHealthOmicsServiceLinkedRolePolicy	2849
Utilisation de cette politique	2849
Détails de la politique	2849
Version de la politique	2849
Document de politique JSON	2849
En savoir plus	2851

AWSIAMIdentityCenterAllowListForIdentityContext	2852
Utilisation de cette politique	2852
Détails de la politique	2852
Version de la politique	2852
Document de politique JSON	2852
En savoir plus	2855
AWSIAMRoleManagerServiceRolePolicy	2856
Utilisation de cette politique	2856
Détails de la politique	2856
Version de la politique	2856
Document de politique JSON	2856
En savoir plus	2857
AWSIdentityCenterExternalManagementPolicy	2857
Utilisation de cette politique	2857
Détails de la politique	2857
Version de la politique	2858
Document de politique JSON	2858
En savoir plus	2859
AWSIdentitySyncFullAccess	2860
Utilisation de cette politique	2860
Détails de la politique	2860
Version de la politique	2860
Document de politique JSON	2860
En savoir plus	2861
AWSIdentitySyncReadOnlyAccess	2861
Utilisation de cette politique	2861
Détails de la politique	2862
Version de la politique	2862
Document de politique JSON	2862
En savoir plus	2862
AWSImageBuilderFullAccess	2863
Utilisation de cette politique	2863
Détails de la politique	2863
Version de la politique	2863
Document de politique JSON	2863
En savoir plus	2866

AWSImageBuilderReadOnlyAccess	2866
Utilisation de cette politique	2866
Détails de la politique	2866
Version de la politique	2867
Document de politique JSON	2867
En savoir plus	2867
AWSImportExportFullAccess	2868
Utilisation de cette politique	2868
Détails de la politique	2868
Version de la politique	2868
Document de politique JSON	2868
En savoir plus	2869
AWSImportExportReadOnlyAccess	2869
Utilisation de cette politique	2869
Détails de la politique	2869
Version de la politique	2869
Document de politique JSON	2869
En savoir plus	2870
AWSIncidentManagerIncidentAccessServiceRolePolicy	2870
Utilisation de cette politique	2870
Détails de la politique	2870
Version de la politique	2871
Document de politique JSON	2871
En savoir plus	2871
AWSIncidentManagerResolverAccess	2872
Utilisation de cette politique	2872
Détails de la politique	2872
Version de la politique	2872
Document de politique JSON	2872
En savoir plus	2873
AWSIncidentManagerServiceRolePolicy	2874
Utilisation de cette politique	2874
Détails de la politique	2874
Version de la politique	2874
Document de politique JSON	2874
En savoir plus	2875

AWSIoT1ClickFullAccess	2876
Utilisation de cette politique	2876
Détails de la politique	2876
Version de la politique	2876
Document de politique JSON	2876
En savoir plus	2877
AWSIoT1ClickReadOnlyAccess	2877
Utilisation de cette politique	2877
Détails de la politique	2877
Version de la politique	2877
Document de politique JSON	2877
En savoir plus	2878
AWSIoTAnalyticsFullAccess	2878
Utilisation de cette politique	2878
Détails de la politique	2878
Version de la politique	2879
Document de politique JSON	2879
En savoir plus	2879
AWSIoTAnalyticsReadOnlyAccess	2879
Utilisation de cette politique	2879
Détails de la politique	2880
Version de la politique	2880
Document de politique JSON	2880
En savoir plus	2880
AWSIoTConfigAccess	2881
Utilisation de cette politique	2881
Détails de la politique	2881
Version de la politique	2881
Document de politique JSON	2881
En savoir plus	2885
AWSIoTConfigReadOnlyAccess	2885
Utilisation de cette politique	2885
Détails de la politique	2886
Version de la politique	2886
Document de politique JSON	2886
En savoir plus	2888

AWSIoTDataAccess	2888
Utilisation de cette politique	2888
Détails de la politique	2888
Version de la politique	2889
Document de politique JSON	2889
En savoir plus	2889
AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction	2890
Utilisation de cette politique	2890
Détails de la politique	2890
Version de la politique	2890
Document de politique JSON	2890
En savoir plus	2891
AWSIoTDeviceDefenderAudit	2891
Utilisation de cette politique	2891
Détails de la politique	2891
Version de la politique	2891
Document de politique JSON	2892
En savoir plus	2893
AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction	2893
Utilisation de cette politique	2893
Détails de la politique	2893
Version de la politique	2893
Document de politique JSON	2894
En savoir plus	2894
AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction	2895
Utilisation de cette politique	2895
Détails de la politique	2895
Version de la politique	2895
Document de politique JSON	2895
En savoir plus	2896
AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction	2896
Utilisation de cette politique	2896
Détails de la politique	2896
Version de la politique	2897
Document de politique JSON	2897
En savoir plus	2897

AWSIoTDeviceDefenderUpdateCACertMitigationAction	2897
Utilisation de cette politique	2898
Détails de la politique	2898
Version de la politique	2898
Document de politique JSON	2898
En savoir plus	2899
AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction	2899
Utilisation de cette politique	2899
Détails de la politique	2899
Version de la politique	2899
Document de politique JSON	2900
En savoir plus	2900
AWSIoTDeviceTesterForFreeRTOSFullAccess	2900
Utilisation de cette politique	2900
Détails de la politique	2900
Version de la politique	2901
Document de politique JSON	2901
En savoir plus	2907
AWSIoTDeviceTesterForGreengrassFullAccess	2907
Utilisation de cette politique	2907
Détails de la politique	2907
Version de la politique	2908
Document de politique JSON	2908
En savoir plus	2911
AWSIoTEventsFullAccess	2911
Utilisation de cette politique	2911
Détails de la politique	2911
Version de la politique	2911
Document de politique JSON	2912
En savoir plus	2912
AWSIoTEventsReadOnlyAccess	2912
Utilisation de cette politique	2912
Détails de la politique	2912
Version de la politique	2913
Document de politique JSON	2913
En savoir plus	2913

AWSIoT FleetHubFederationAccess	2913
Utilisation de cette politique	2913
Détails de la politique	2914
Version de la politique	2914
Document de politique JSON	2914
En savoir plus	2916
AWSIoT FleetwiseServiceRolePolicy	2916
Utilisation de cette politique	2916
Détails de la politique	2916
Version de la politique	2916
Document de politique JSON	2917
En savoir plus	2917
AWSIoT FullAccess	2917
Utilisation de cette politique	2918
Détails de la politique	2918
Version de la politique	2918
Document de politique JSON	2918
En savoir plus	2918
AWSIoT Logging	2919
Utilisation de cette politique	2919
Détails de la politique	2919
Version de la politique	2919
Document de politique JSON	2919
En savoir plus	2920
AWSIoT ManagedIntegrationsFullAccess	2920
Utilisation de cette politique	2920
Détails de la politique	2920
Version de la politique	2921
Document de politique JSON	2921
En savoir plus	2921
AWSIoT ManagedIntegrationsRolePolicy	2922
Utilisation de cette politique	2922
Détails de la politique	2922
Version de la politique	2922
Document de politique JSON	2922
En savoir plus	2924

AWSIoTOTAUpdate	2924
Utilisation de cette politique	2924
Détails de la politique	2924
Version de la politique	2924
Document de politique JSON	2924
En savoir plus	2925
AWSIoTRoboRunnerFullAccess	2925
Utilisation de cette politique	2925
Détails de la politique	2925
Version de la politique	2925
Document de politique JSON	2926
En savoir plus	2926
AWSIoTRoboRunnerReadOnly	2926
Utilisation de cette politique	2927
Détails de la politique	2927
Version de la politique	2927
Document de politique JSON	2927
En savoir plus	2928
AWSIoTRoboRunnerServiceRolePolicy	2928
Utilisation de cette politique	2928
Détails de la politique	2928
Version de la politique	2928
Document de politique JSON	2929
En savoir plus	2929
AWSIoTRuleActions	2929
Utilisation de cette politique	2929
Détails de la politique	2929
Version de la politique	2930
Document de politique JSON	2930
En savoir plus	2930
AWSIoTSiteWiseConsoleFullAccess	2931
Utilisation de cette politique	2931
Détails de la politique	2931
Version de la politique	2931
Document de politique JSON	2931
En savoir plus	2933

AWSIoTSiteWiseFullAccess	2934
Utilisation de cette politique	2934
Détails de la politique	2934
Version de la politique	2934
Document de politique JSON	2934
En savoir plus	2935
AWSIoTSiteWiseMonitorPortalAccess	2935
Utilisation de cette politique	2935
Détails de la politique	2935
Version de la politique	2935
Document de politique JSON	2936
En savoir plus	2937
AWSIoTSiteWiseMonitorServiceRolePolicy	2937
Utilisation de cette politique	2937
Détails de la politique	2937
Version de la politique	2937
Document de politique JSON	2938
En savoir plus	2939
AWSIoTSiteWiseReadOnlyAccess	2939
Utilisation de cette politique	2939
Détails de la politique	2939
Version de la politique	2939
Document de politique JSON	2939
En savoir plus	2941
AWSIoTThingsRegistration	2941
Utilisation de cette politique	2941
Détails de la politique	2941
Version de la politique	2942
Document de politique JSON	2942
En savoir plus	2943
AWSIoTTwinMakerServiceRolePolicy	2943
Utilisation de cette politique	2943
Détails de la politique	2943
Version de la politique	2944
Document de politique JSON	2944
En savoir plus	2945

AWSIoTWirelessDataAccess	2946
Utilisation de cette politique	2946
Détails de la politique	2946
Version de la politique	2946
Document de politique JSON	2946
En savoir plus	2947
AWSIoTWirelessFullAccess	2947
Utilisation de cette politique	2947
Détails de la politique	2947
Version de la politique	2947
Document de politique JSON	2947
En savoir plus	2948
AWSIoTWirelessFullPublishAccess	2948
Utilisation de cette politique	2948
Détails de la politique	2948
Version de la politique	2949
Document de politique JSON	2949
En savoir plus	2949
AWSIoTWirelessGatewayCertManager	2949
Utilisation de cette politique	2949
Détails de la politique	2950
Version de la politique	2950
Document de politique JSON	2950
En savoir plus	2950
AWSIoTWirelessLogging	2951
Utilisation de cette politique	2951
Détails de la politique	2951
Version de la politique	2951
Document de politique JSON	2951
En savoir plus	2952
AWSIoTWirelessReadOnlyAccess	2952
Utilisation de cette politique	2952
Détails de la politique	2952
Version de la politique	2952
Document de politique JSON	2953
En savoir plus	2953

AWSIPAMServiceRolePolicy	2953
Utilisation de cette politique	2953
Détails de la politique	2954
Version de la politique	2954
Document de politique JSON	2954
En savoir plus	2956
AWSIQContractServiceRolePolicy	2956
Utilisation de cette politique	2956
Détails de la politique	2956
Version de la politique	2957
Document de politique JSON	2957
En savoir plus	2957
AWSIQFullAccess	2957
Utilisation de cette politique	2958
Détails de la politique	2958
Version de la politique	2958
Document de politique JSON	2958
En savoir plus	2959
AWSIQPermissionServiceRolePolicy	2959
Utilisation de cette politique	2959
Détails de la politique	2959
Version de la politique	2959
Document de politique JSON	2960
En savoir plus	2960
AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy	2961
Utilisation de cette politique	2961
Détails de la politique	2961
Version de la politique	2961
Document de politique JSON	2961
En savoir plus	2962
AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy	2962
Utilisation de cette politique	2962
Détails de la politique	2962
Version de la politique	2963
Document de politique JSON	2963
En savoir plus	2963

AWSKeyManagementServicePowerUser	2963
Utilisation de cette politique	2964
Détails de la politique	2964
Version de la politique	2964
Document de politique JSON	2964
En savoir plus	2965
AWSLakeFormationCrossAccountManager	2965
Utilisation de cette politique	2965
Détails de la politique	2965
Version de la politique	2965
Document de politique JSON	2966
En savoir plus	2968
AWSLakeFormationDataAdmin	2968
Utilisation de cette politique	2968
Détails de la politique	2968
Version de la politique	2968
Document de politique JSON	2968
En savoir plus	2970
AWSLambda_FullAccess	2970
Utilisation de cette politique	2970
Détails de la politique	2970
Version de la politique	2971
Document de politique JSON	2971
En savoir plus	2972
AWSLambda_ReadOnlyAccess	2973
Utilisation de cette politique	2973
Détails de la politique	2973
Version de la politique	2973
Document de politique JSON	2973
En savoir plus	2975
AWSLambdaBasicDurableExecutionRolePolicy	2975
Utilisation de cette politique	2975
Détails de la politique	2975
Version de la politique	2975
Document de politique JSON	2976
En savoir plus	2976

AWSLambdaBasicExecutionRole	2976
Utilisation de cette politique	2976
Détails de la politique	2976
Version de la politique	2977
Document de politique JSON	2977
En savoir plus	2977
AWSLambdaDynamoDBExecutionRole	2978
Utilisation de cette politique	2978
Détails de la politique	2978
Version de la politique	2978
Document de politique JSON	2978
En savoir plus	2979
AWSLambdaENIManagementAccess	2979
Utilisation de cette politique	2979
Détails de la politique	2979
Version de la politique	2979
Document de politique JSON	2980
En savoir plus	2980
AWSLambdaExecute	2980
Utilisation de cette politique	2981
Détails de la politique	2981
Version de la politique	2981
Document de politique JSON	2981
En savoir plus	2982
AWSLambdaFullAccess	2982
Utilisation de cette politique	2982
Détails de la politique	2982
Version de la politique	2983
Document de politique JSON	2983
En savoir plus	2984
AWSLambdaInvocation-DynamoDB	2984
Utilisation de cette politique	2985
Détails de la politique	2985
Version de la politique	2985
Document de politique JSON	2985
En savoir plus	2986

AWSLambdaInvokeWebFunctionEndpointAccess	2986
Utilisation de cette politique	2986
Détails de la politique	2986
Version de la politique	2986
Document de politique JSON	2987
En savoir plus	2987
AWSLambdaKinesisExecutionRole	2987
Utilisation de cette politique	2987
Détails de la politique	2988
Version de la politique	2988
Document de politique JSON	2988
En savoir plus	2989
AWSLambdaManagedEC2ResourceOperator	2989
Utilisation de cette politique	2989
Détails de la politique	2989
Version de la politique	2989
Document de politique JSON	2989
En savoir plus	2991
AWSLambdaMSKExecutionRole	2992
Utilisation de cette politique	2992
Détails de la politique	2992
Version de la politique	2992
Document de politique JSON	2992
En savoir plus	2993
AWSLambdaNetworkConnectorOperatorPolicy	2993
Utilisation de cette politique	2993
Détails de la politique	2993
Version de la politique	2994
Document de politique JSON	2994
En savoir plus	2995
AWSLambdaReplicator	2995
Utilisation de cette politique	2995
Détails de la politique	2995
Version de la politique	2996
Document de politique JSON	2996
En savoir plus	2997

AWSLambdaRole	2997
Utilisation de cette politique	2997
Détails de la politique	2997
Version de la politique	2997
Document de politique JSON	2998
En savoir plus	2998
AWSLambdaServiceRolePolicy	2998
Utilisation de cette politique	2998
Détails de la politique	2998
Version de la politique	2999
Document de politique JSON	2999
En savoir plus	3000
AWSLambdaSQSQueueExecutionRole	3000
Utilisation de cette politique	3000
Détails de la politique	3001
Version de la politique	3001
Document de politique JSON	3001
En savoir plus	3001
AWSLambdaVPCLAccessExecutionRole	3002
Utilisation de cette politique	3002
Détails de la politique	3002
Version de la politique	3002
Document de politique JSON	3002
En savoir plus	3003
AWSLicenseManagerConsumptionPolicy	3003
Utilisation de cette politique	3003
Détails de la politique	3003
Version de la politique	3004
Document de politique JSON	3004
En savoir plus	3004
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy	3005
Utilisation de cette politique	3005
Détails de la politique	3005
Version de la politique	3005
Document de politique JSON	3005
En savoir plus	3007

AWSLicenseManagerMasterAccountRolePolicy	3007
Utilisation de cette politique	3007
Détails de la politique	3007
Version de la politique	3008
Document de politique JSON	3008
En savoir plus	3013
AWSLicenseManagerMemberAccountRolePolicy	3013
Utilisation de cette politique	3013
Détails de la politique	3013
Version de la politique	3013
Document de politique JSON	3013
En savoir plus	3015
AWSLicenseManagerServiceRolePolicy	3015
Utilisation de cette politique	3015
Détails de la politique	3015
Version de la politique	3015
Document de politique JSON	3015
En savoir plus	3019
AWSLicenseManagerUserSubscriptionsServiceRolePolicy	3019
Utilisation de cette politique	3019
Détails de la politique	3019
Version de la politique	3020
Document de politique JSON	3020
En savoir plus	3023
AWSM2ServicePolicy	3023
Utilisation de cette politique	3023
Détails de la politique	3023
Version de la politique	3024
Document de politique JSON	3024
En savoir plus	3025
AWSManagedAccountManagementAccess	3025
Utilisation de cette politique	3025
Détails de la politique	3025
Version de la politique	3026
Document de politique JSON	3026
En savoir plus	3027

AWSManagedAccountUserEntitlementAccess	3027
Utilisation de cette politique	3027
Détails de la politique	3027
Version de la politique	3027
Document de politique JSON	3028
En savoir plus	3028
AWSManagedAdvancedFeaturesActivationAccess	3028
Utilisation de cette politique	3029
Détails de la politique	3029
Version de la politique	3029
Document de politique JSON	3029
En savoir plus	3029
AWSManagedBudgetsSpendLimitManagementAccess	3030
Utilisation de cette politique	3030
Détails de la politique	3030
Version de la politique	3030
Document de politique JSON	3030
En savoir plus	3031
AWSManagedControlPolicyManagementAccess	3032
Utilisation de cette politique	3032
Détails de la politique	3032
Version de la politique	3032
Document de politique JSON	3032
En savoir plus	3033
AWSManagedServiceAccessManagementAccess	3033
Utilisation de cette politique	3033
Détails de la politique	3033
Version de la politique	3034
Document de politique JSON	3034
En savoir plus	3035
AWSManagedServices_ContactsServiceRolePolicy	3036
Utilisation de cette politique	3036
Détails de la politique	3036
Version de la politique	3036
Document de politique JSON	3036
En savoir plus	3037

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy	3037
Utilisation de cette politique	3037
Détails de la politique	3037
Version de la politique	3038
Document de politique JSON	3038
En savoir plus	3039
AWSManagedServices_EventsServiceRolePolicy	3040
Utilisation de cette politique	3040
Détails de la politique	3040
Version de la politique	3040
Document de politique JSON	3040
En savoir plus	3041
AWSManagedServices_SelfServiceReporting_ServiceRolePolicy	3041
Utilisation de cette politique	3041
Détails de la politique	3042
Version de la politique	3042
Document de politique JSON	3042
En savoir plus	3042
AWSManagedServicesDeploymentToolkitPolicy	3043
Utilisation de cette politique	3043
Détails de la politique	3043
Version de la politique	3043
Document de politique JSON	3043
En savoir plus	3045
AWSManagedSettingsAdminAccess	3046
Utilisation de cette politique	3046
Détails de la politique	3046
Version de la politique	3046
Document de politique JSON	3046
En savoir plus	3057
AWSManagedSettingsReadOnlyAccess	3057
Utilisation de cette politique	3057
Détails de la politique	3057
Version de la politique	3057
Document de politique JSON	3058
En savoir plus	3059

AWSManagedSignUpAdminAccess	3059
Utilisation de cette politique	3059
Détails de la politique	3059
Version de la politique	3060
Document de politique JSON	3060
En savoir plus	3061
AWSManagementConsoleAdministratorAccess	3062
Utilisation de cette politique	3062
Détails de la politique	3062
Version de la politique	3062
Document de politique JSON	3062
En savoir plus	3065
AWSManagementConsoleBasicUserAccess	3065
Utilisation de cette politique	3065
Détails de la politique	3065
Version de la politique	3065
Document de politique JSON	3066
En savoir plus	3067
AWSMarketplaceAmiIngestion	3067
Utilisation de cette politique	3067
Détails de la politique	3067
Version de la politique	3067
Document de politique JSON	3067
En savoir plus	3068
AWSMarketplaceDeploymentServiceRolePolicy	3068
Utilisation de cette politique	3068
Détails de la politique	3069
Version de la politique	3069
Document de politique JSON	3069
En savoir plus	3070
AWSMarketplaceDiscoveryFullAccess	3071
Utilisation de cette politique	3071
Détails de la politique	3071
Version de la politique	3071
Document de politique JSON	3071
En savoir plus	3072

AWSMarketplaceFullAccess	3072
Utilisation de cette politique	3072
Détails de la politique	3072
Version de la politique	3073
Document de politique JSON	3073
En savoir plus	3075
AWSMarketplaceGetEntitlements	3075
Utilisation de cette politique	3076
Détails de la politique	3076
Version de la politique	3076
Document de politique JSON	3076
En savoir plus	3076
AWSMarketplaceImageBuildFullAccess	3077
Utilisation de cette politique	3077
Détails de la politique	3077
Version de la politique	3077
Document de politique JSON	3077
En savoir plus	3081
AWSMarketplaceLicenseManagementServiceRolePolicy	3081
Utilisation de cette politique	3081
Détails de la politique	3081
Version de la politique	3082
Document de politique JSON	3082
En savoir plus	3082
AWSMarketplaceManageSubscriptions	3083
Utilisation de cette politique	3083
Détails de la politique	3083
Version de la politique	3083
Document de politique JSON	3083
En savoir plus	3086
AWSMarketplaceMeteringFullAccess	3087
Utilisation de cette politique	3087
Détails de la politique	3087
Version de la politique	3087
Document de politique JSON	3087
En savoir plus	3088

AWSMarketplaceMeteringRegisterUsage	3088
Utilisation de cette politique	3088
Détails de la politique	3088
Version de la politique	3088
Document de politique JSON	3089
En savoir plus	3089
AWSMarketplaceProcurementSystemAdminFullAccess	3089
Utilisation de cette politique	3089
Détails de la politique	3089
Version de la politique	3090
Document de politique JSON	3090
En savoir plus	3090
AWSMarketplacePurchaseOrdersServiceRolePolicy	3091
Utilisation de cette politique	3091
Détails de la politique	3091
Version de la politique	3091
Document de politique JSON	3091
En savoir plus	3092
AWSMarketplaceRead-only	3092
Utilisation de cette politique	3092
Détails de la politique	3092
Version de la politique	3092
Document de politique JSON	3093
En savoir plus	3095
AWSMarketplaceResaleAuthorizationServiceRolePolicy	3095
Utilisation de cette politique	3095
Détails de la politique	3095
Version de la politique	3095
Document de politique JSON	3096
En savoir plus	3098
AWSMarketplaceSellerFullAccess	3098
Utilisation de cette politique	3098
Détails de la politique	3098
Version de la politique	3098
Document de politique JSON	3099
En savoir plus	3106

AWSMarketplaceSellerOfferManagement	3106
Utilisation de cette politique	3106
Détails de la politique	3106
Version de la politique	3106
Document de politique JSON	3107
En savoir plus	3109
AWSMarketplaceSellerProductsFullAccess	3109
Utilisation de cette politique	3109
Détails de la politique	3110
Version de la politique	3110
Document de politique JSON	3110
En savoir plus	3113
AWSMarketplaceSellerProductsReadOnly	3113
Utilisation de cette politique	3114
Détails de la politique	3114
Version de la politique	3114
Document de politique JSON	3114
En savoir plus	3115
AWSMcpServiceActionsFullAccess	3115
Utilisation de cette politique	3115
Détails de la politique	3115
Version de la politique	3116
Document de politique JSON	3116
En savoir plus	3116
AWSMCPSignInOAuthAccessPolicy	3117
Utilisation de cette politique	3117
Détails de la politique	3117
Version de la politique	3117
Document de politique JSON	3117
En savoir plus	3118
AWSMediaConnectServicePolicy	3118
Utilisation de cette politique	3118
Détails de la politique	3118
Version de la politique	3118
Document de politique JSON	3119
En savoir plus	3120

AWSMediaLiveAnywhereServiceRolePolicy	3121
Utilisation de cette politique	3121
Détails de la politique	3121
Version de la politique	3121
Document de politique JSON	3121
En savoir plus	3124
AWSMediaTailorServiceRolePolicy	3124
Utilisation de cette politique	3124
Détails de la politique	3125
Version de la politique	3125
Document de politique JSON	3125
En savoir plus	3126
AWSMigrationHubDiscoveryAccess	3126
Utilisation de cette politique	3126
Détails de la politique	3126
Version de la politique	3126
Document de politique JSON	3126
En savoir plus	3128
AWSMigrationHubDMSAccess	3128
Utilisation de cette politique	3128
Détails de la politique	3128
Version de la politique	3128
Document de politique JSON	3129
En savoir plus	3130
AWSMigrationHubFullAccess	3130
Utilisation de cette politique	3130
Détails de la politique	3130
Version de la politique	3130
Document de politique JSON	3130
En savoir plus	3132
AWSMigrationHubOrchestratorConsoleFullAccess	3132
Utilisation de cette politique	3132
Détails de la politique	3132
Version de la politique	3133
Document de politique JSON	3133
En savoir plus	3136

AWSMigrationHubOrchestratorInstanceRolePolicy	3136
Utilisation de cette politique	3136
Détails de la politique	3136
Version de la politique	3137
Document de politique JSON	3137
En savoir plus	3137
AWSMigrationHubOrchestratorPlugin	3138
Utilisation de cette politique	3138
Détails de la politique	3138
Version de la politique	3138
Document de politique JSON	3138
En savoir plus	3139
AWSMigrationHubOrchestratorServiceRolePolicy	3140
Utilisation de cette politique	3140
Détails de la politique	3140
Version de la politique	3140
Document de politique JSON	3140
En savoir plus	3144
AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess	3144
Utilisation de cette politique	3144
Détails de la politique	3144
Version de la politique	3145
Document de politique JSON	3145
En savoir plus	3150
AWSMigrationHubRefactorSpaces-SSMAutomationPolicy	3151
Utilisation de cette politique	3151
Détails de la politique	3151
Version de la politique	3151
Document de politique JSON	3151
En savoir plus	3153
AWSMigrationHubRefactorSpacesFullAccess	3153
Utilisation de cette politique	3153
Détails de la politique	3153
Version de la politique	3154
Document de politique JSON	3154
En savoir plus	3160

AWSMigrationHubRefactorSpacesServiceRolePolicy	3160
Utilisation de cette politique	3161
Détails de la politique	3161
Version de la politique	3161
Document de politique JSON	3161
En savoir plus	3165
AWSMigrationHubSMSAccess	3165
Utilisation de cette politique	3165
Détails de la politique	3165
Version de la politique	3165
Document de politique JSON	3166
En savoir plus	3167
AWSMigrationHubStrategyCollector	3167
Utilisation de cette politique	3167
Détails de la politique	3167
Version de la politique	3167
Document de politique JSON	3168
En savoir plus	3170
AWSMigrationHubStrategyConsoleFullAccess	3170
Utilisation de cette politique	3170
Détails de la politique	3170
Version de la politique	3171
Document de politique JSON	3171
En savoir plus	3172
AWSMigrationHubStrategyServiceRolePolicy	3173
Utilisation de cette politique	3173
Détails de la politique	3173
Version de la politique	3173
Document de politique JSON	3173
En savoir plus	3174
AWSMobileHub_FullAccess	3174
Utilisation de cette politique	3175
Détails de la politique	3175
Version de la politique	3175
Document de politique JSON	3175
En savoir plus	3177

AWSMobileHub_ReadOnly	3177
Utilisation de cette politique	3177
Détails de la politique	3177
Version de la politique	3177
Document de politique JSON	3178
En savoir plus	3179
AWSMSKReplicatorExecutionRole	3179
Utilisation de cette politique	3179
Détails de la politique	3179
Version de la politique	3179
Document de politique JSON	3180
En savoir plus	3181
AWSNATGatewayServiceRolePolicy	3181
Utilisation de cette politique	3181
Détails de la politique	3181
Version de la politique	3182
Document de politique JSON	3182
En savoir plus	3182
AWSNetworkFirewallFullAccess	3182
Utilisation de cette politique	3183
Détails de la politique	3183
Version de la politique	3183
Document de politique JSON	3183
En savoir plus	3187
AWSNetworkFirewallReadOnlyAccess	3187
Utilisation de cette politique	3187
Détails de la politique	3188
Version de la politique	3188
Document de politique JSON	3188
En savoir plus	3189
AWSNetworkFirewallServiceRolePolicy	3189
Utilisation de cette politique	3190
Détails de la politique	3190
Version de la politique	3190
Document de politique JSON	3190
En savoir plus	3192

AWSNetworkManagerCloudWANServiceRolePolicy	3192
Utilisation de cette politique	3192
Détails de la politique	3192
Version de la politique	3193
Document de politique JSON	3193
En savoir plus	3193
AWSNetworkManagerFullAccess	3193
Utilisation de cette politique	3193
Détails de la politique	3194
Version de la politique	3194
Document de politique JSON	3194
En savoir plus	3195
AWSNetworkManagerReadOnlyAccess	3195
Utilisation de cette politique	3195
Détails de la politique	3195
Version de la politique	3195
Document de politique JSON	3195
En savoir plus	3196
AWSNetworkManagerServiceRolePolicy	3196
Utilisation de cette politique	3196
Détails de la politique	3196
Version de la politique	3197
Document de politique JSON	3197
En savoir plus	3198
AWSObservabilityAdminLogsCentralizationServiceRolePolicy	3198
Utilisation de cette politique	3198
Détails de la politique	3198
Version de la politique	3198
Document de politique JSON	3199
En savoir plus	3199
AWSObservabilityAdminServiceRolePolicy	3200
Utilisation de cette politique	3200
Détails de la politique	3200
Version de la politique	3200
Document de politique JSON	3200
En savoir plus	3203

AWSObservabilityAdminTelemetryEnablementServiceRolePolicy	3203
Utilisation de cette politique	3203
Détails de la politique	3203
Version de la politique	3204
Document de politique JSON	3204
En savoir plus	3221
AWSOrganizationsFullAccess	3221
Utilisation de cette politique	3221
Détails de la politique	3221
Version de la politique	3222
Document de politique JSON	3222
En savoir plus	3223
AWSOrganizationsReadOnlyAccess	3223
Utilisation de cette politique	3223
Détails de la politique	3223
Version de la politique	3223
Document de politique JSON	3224
En savoir plus	3224
AWSOrganizationsServiceTrustPolicy	3225
Utilisation de cette politique	3225
Détails de la politique	3225
Version de la politique	3225
Document de politique JSON	3225
En savoir plus	3226
AWSOutpostsAuthorizeServerPolicy	3226
Utilisation de cette politique	3226
Détails de la politique	3226
Version de la politique	3227
Document de politique JSON	3227
En savoir plus	3227
AWSOutpostsServiceRolePolicy	3227
Utilisation de cette politique	3228
Détails de la politique	3228
Version de la politique	3228
Document de politique JSON	3228
En savoir plus	3230

AWSPanoramaApplianceRolePolicy	3230
Utilisation de cette politique	3230
Détails de la politique	3230
Version de la politique	3231
Document de politique JSON	3231
En savoir plus	3231
AWSPanoramaApplianceServiceRolePolicy	3232
Utilisation de cette politique	3232
Détails de la politique	3232
Version de la politique	3232
Document de politique JSON	3232
En savoir plus	3234
AWSPanoramaFullAccess	3234
Utilisation de cette politique	3234
Détails de la politique	3234
Version de la politique	3234
Document de politique JSON	3235
En savoir plus	3237
AWSPanoramaGreengrassGroupRolePolicy	3237
Utilisation de cette politique	3237
Détails de la politique	3238
Version de la politique	3238
Document de politique JSON	3238
En savoir plus	3239
AWSPanoramaSageMakerRolePolicy	3240
Utilisation de cette politique	3240
Détails de la politique	3240
Version de la politique	3240
Document de politique JSON	3240
En savoir plus	3241
AWSPanoramaServiceLinkedRolePolicy	3241
Utilisation de cette politique	3241
Détails de la politique	3241
Version de la politique	3241
Document de politique JSON	3242
En savoir plus	3244

AWSPanoramaServiceRolePolicy	3244
Utilisation de cette politique	3245
Détails de la politique	3245
Version de la politique	3245
Document de politique JSON	3245
En savoir plus	3252
AWSPartnerCentralChannelHandshakeApprovalManagement	3252
Utilisation de cette politique	3252
Détails de la politique	3252
Version de la politique	3253
Document de politique JSON	3253
En savoir plus	3254
AWSPartnerCentralChannelManagement	3254
Utilisation de cette politique	3254
Détails de la politique	3254
Version de la politique	3254
Document de politique JSON	3254
En savoir plus	3257
AWSPartnerCentralFullAccess	3258
Utilisation de cette politique	3258
Détails de la politique	3258
Version de la politique	3258
Document de politique JSON	3258
En savoir plus	3263
AWSPartnerCentralMarketingManagement	3263
Utilisation de cette politique	3263
Détails de la politique	3263
Version de la politique	3263
Document de politique JSON	3263
En savoir plus	3266
AWSPartnerCentralOpportunityManagement	3266
Utilisation de cette politique	3266
Détails de la politique	3266
Version de la politique	3267
Document de politique JSON	3267
En savoir plus	3271

AWSPartnerCentralRevenueAttributionManagement	3271
Utilisation de cette politique	3272
Détails de la politique	3272
Version de la politique	3272
Document de politique JSON	3272
En savoir plus	3277
AWSPartnerCentralSandboxFullAccess	3277
Utilisation de cette politique	3277
Détails de la politique	3277
Version de la politique	3277
Document de politique JSON	3278
En savoir plus	3279
AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy	3279
Utilisation de cette politique	3279
Détails de la politique	3279
Version de la politique	3280
Document de politique JSON	3280
En savoir plus	3280
AWSPartnerLedSupportReadOnlyAccess	3281
Utilisation de cette politique	3281
Détails de la politique	3281
Version de la politique	3281
Document de politique JSON	3281
En savoir plus	3318
AWSPartnerProServeToolsFullAccess	3318
Utilisation de cette politique	3319
Détails de la politique	3319
Version de la politique	3319
Document de politique JSON	3319
En savoir plus	3320
AWSPartnerProServeToolsIndividualContributor	3320
Utilisation de cette politique	3320
Détails de la politique	3320
Version de la politique	3320
Document de politique JSON	3321
En savoir plus	3321

AWSPartnerProServeToolsOrganizationReaderIndividualContributor	3321
Utilisation de cette politique	3322
Détails de la politique	3322
Version de la politique	3322
Document de politique JSON	3322
En savoir plus	3323
AWSPCSCComputeNodePolicy	3323
Utilisation de cette politique	3323
Détails de la politique	3323
Version de la politique	3323
Document de politique JSON	3324
En savoir plus	3324
AWSPCSServiceRolePolicy	3324
Utilisation de cette politique	3324
Détails de la politique	3324
Version de la politique	3325
Document de politique JSON	3325
En savoir plus	3330
AWSPriceListServiceFullAccess	3330
Utilisation de cette politique	3330
Détails de la politique	3330
Version de la politique	3330
Document de politique JSON	3331
En savoir plus	3331
AWSPprivateCAAuditor	3331
Utilisation de cette politique	3331
Détails de la politique	3331
Version de la politique	3332
Document de politique JSON	3332
En savoir plus	3333
AWSPprivateCAConnectorForKubernetesPolicy	3333
Utilisation de cette politique	3333
Détails de la politique	3333
Version de la politique	3333
Document de politique JSON	3333
En savoir plus	3334

AWSPriateCAFullAccess	3334
Utilisation de cette politique	3334
Détails de la politique	3334
Version de la politique	3335
Document de politique JSON	3335
En savoir plus	3335
AWSPriateCAPrivilegedUser	3335
Utilisation de cette politique	3336
Détails de la politique	3336
Version de la politique	3336
Document de politique JSON	3336
En savoir plus	3337
AWSPriateCAReadOnly	3337
Utilisation de cette politique	3338
Détails de la politique	3338
Version de la politique	3338
Document de politique JSON	3338
En savoir plus	3339
AWSPriateCAUser	3339
Utilisation de cette politique	3339
Détails de la politique	3339
Version de la politique	3339
Document de politique JSON	3339
En savoir plus	3341
AWSPriateMarketplaceAdminFullAccess	3341
Utilisation de cette politique	3341
Détails de la politique	3341
Version de la politique	3341
Document de politique JSON	3342
En savoir plus	3344
AWSPriateMarketplaceRequests	3344
Utilisation de cette politique	3345
Détails de la politique	3345
Version de la politique	3345
Document de politique JSON	3345
En savoir plus	3347

AWSPprivateNetworksServiceRolePolicy	3347
Utilisation de cette politique	3347
Détails de la politique	3347
Version de la politique	3348
Document de politique JSON	3348
En savoir plus	3348
AWSPProtonCodeBuildProvisioningBasicAccess	3349
Utilisation de cette politique	3349
Détails de la politique	3349
Version de la politique	3349
Document de politique JSON	3349
En savoir plus	3350
AWSPProtonCodeBuildProvisioningServiceRolePolicy	3350
Utilisation de cette politique	3350
Détails de la politique	3350
Version de la politique	3351
Document de politique JSON	3351
En savoir plus	3352
AWSPProtonDeveloperAccess	3352
Utilisation de cette politique	3352
Détails de la politique	3352
Version de la politique	3353
Document de politique JSON	3353
En savoir plus	3355
AWSPProtonFullAccess	3355
Utilisation de cette politique	3356
Détails de la politique	3356
Version de la politique	3356
Document de politique JSON	3356
En savoir plus	3358
AWSPProtonReadOnlyAccess	3358
Utilisation de cette politique	3358
Détails de la politique	3359
Version de la politique	3359
Document de politique JSON	3359
En savoir plus	3360

AWSProtonServiceGitSyncServiceRolePolicy	3361
Utilisation de cette politique	3361
Détails de la politique	3361
Version de la politique	3361
Document de politique JSON	3361
En savoir plus	3362
AWSProtonSyncServiceRolePolicy	3362
Utilisation de cette politique	3362
Détails de la politique	3362
Version de la politique	3363
Document de politique JSON	3363
En savoir plus	3364
AWSPurchaseOrdersServiceRolePolicy	3364
Utilisation de cette politique	3364
Détails de la politique	3364
Version de la politique	3365
Document de politique JSON	3365
En savoir plus	3366
AWSQuickSetupCFGCPacksPermissionsBoundary	3366
Utilisation de cette politique	3366
Détails de la politique	3366
Version de la politique	3366
Document de politique JSON	3367
En savoir plus	3369
AWSQuickSetupDeploymentRolePolicy	3370
Utilisation de cette politique	3370
Détails de la politique	3370
Version de la politique	3370
Document de politique JSON	3370
En savoir plus	3379
AWSQuickSetupDevOpsGuruPermissionsBoundary	3379
Utilisation de cette politique	3380
Détails de la politique	3380
Version de la politique	3380
Document de politique JSON	3380
En savoir plus	3383

AWSQuickSetupDistributorPermissionsBoundary	3383
Utilisation de cette politique	3383
Détails de la politique	3383
Version de la politique	3384
Document de politique JSON	3384
En savoir plus	3389
AWSQuickSetupEnableAREXExecutionPolicy	3390
Utilisation de cette politique	3390
Détails de la politique	3390
Version de la politique	3390
Document de politique JSON	3390
En savoir plus	3392
AWSQuickSetupEnableDHMCEExecutionPolicy	3392
Utilisation de cette politique	3392
Détails de la politique	3392
Version de la politique	3393
Document de politique JSON	3393
En savoir plus	3394
AWSQuickSetupJITNADeploymentRolePolicy	3394
Utilisation de cette politique	3394
Détails de la politique	3394
Version de la politique	3395
Document de politique JSON	3395
En savoir plus	3399
AWSQuickSetupManagedInstanceProfileExecutionPolicy	3399
Utilisation de cette politique	3399
Détails de la politique	3399
Version de la politique	3399
Document de politique JSON	3400
En savoir plus	3404
AWSQuickSetupManageJITNAResourcesExecutionPolicy	3405
Utilisation de cette politique	3405
Détails de la politique	3405
Version de la politique	3405
Document de politique JSON	3405
En savoir plus	3407

AWSQuickSetupPatchPolicyBaselineAccess	3408
Utilisation de cette politique	3408
Détails de la politique	3408
Version de la politique	3408
Document de politique JSON	3408
En savoir plus	3409
AWSQuickSetupPatchPolicyDeploymentRolePolicy	3409
Utilisation de cette politique	3409
Détails de la politique	3410
Version de la politique	3410
Document de politique JSON	3410
En savoir plus	3418
AWSQuickSetupPatchPolicyLambdaExecutionPolicy	3419
Utilisation de cette politique	3419
Détails de la politique	3419
Version de la politique	3419
Document de politique JSON	3419
En savoir plus	3420
AWSQuickSetupPatchPolicyPermissionsBoundary	3420
Utilisation de cette politique	3421
Détails de la politique	3421
Version de la politique	3421
Document de politique JSON	3421
En savoir plus	3429
AWSQuickSetupPatchPolicyTagManagementExecutionPolicy	3430
Utilisation de cette politique	3430
Détails de la politique	3430
Version de la politique	3430
Document de politique JSON	3430
En savoir plus	3431
AWSQuickSetupSchedulerPermissionsBoundary	3432
Utilisation de cette politique	3432
Détails de la politique	3432
Version de la politique	3432
Document de politique JSON	3432
En savoir plus	3436

AWSQuickSetupSSMDeploymentRolePolicy	3436
Utilisation de cette politique	3436
Détails de la politique	3436
Version de la politique	3436
Document de politique JSON	3436
En savoir plus	3448
AWSQuickSetupSSMDeploymentS3BucketRolePolicy	3448
Utilisation de cette politique	3448
Détails de la politique	3448
Version de la politique	3448
Document de politique JSON	3449
En savoir plus	3449
AWSQuickSetupSSMHostMgmtPermissionsBoundary	3450
Utilisation de cette politique	3450
Détails de la politique	3450
Version de la politique	3450
Document de politique JSON	3450
En savoir plus	3456
AWSQuickSetupSSMLifecycleManagementExecutionPolicy	3456
Utilisation de cette politique	3457
Détails de la politique	3457
Version de la politique	3457
Document de politique JSON	3457
En savoir plus	3458
AWSQuickSetupSSMManageResourcesExecutionPolicy	3459
Utilisation de cette politique	3459
Détails de la politique	3459
Version de la politique	3459
Document de politique JSON	3459
En savoir plus	3462
AWSQuickSetupStartSSMAssociationsExecutionPolicy	3462
Utilisation de cette politique	3462
Détails de la politique	3463
Version de la politique	3463
Document de politique JSON	3463
En savoir plus	3464

AWSQuickSetupStartStopInstancesExecutionPolicy	3464
Utilisation de cette politique	3464
Détails de la politique	3465
Version de la politique	3465
Document de politique JSON	3465
En savoir plus	3467
AWSQuickSightAssetBundleExportPolicy	3467
Utilisation de cette politique	3467
Détails de la politique	3467
Version de la politique	3467
Document de politique JSON	3467
En savoir plus	3470
AWSQuickSightAssetBundleImportPolicy	3470
Utilisation de cette politique	3470
Détails de la politique	3470
Version de la politique	3470
Document de politique JSON	3470
En savoir plus	3473
AWSQuickSightAthenaAccess	3474
Utilisation de cette politique	3474
Détails de la politique	3474
Version de la politique	3474
Document de politique JSON	3474
En savoir plus	3476
AWSQuickSightDescribeRDS	3477
Utilisation de cette politique	3477
Détails de la politique	3477
Version de la politique	3477
Document de politique JSON	3477
En savoir plus	3478
AWSQuickSightDescribeRedshift	3478
Utilisation de cette politique	3478
Détails de la politique	3478
Version de la politique	3478
Document de politique JSON	3479
En savoir plus	3479

AWSQuickSightElasticsearchPolicy	3479
Utilisation de cette politique	3479
Détails de la politique	3479
Version de la politique	3480
Document de politique JSON	3480
En savoir plus	3481
AWSQuickSightIoTAnalyticsAccess	3481
Utilisation de cette politique	3481
Détails de la politique	3481
Version de la politique	3482
Document de politique JSON	3482
En savoir plus	3482
AWSQuickSightListIAM	3482
Utilisation de cette politique	3483
Détails de la politique	3483
Version de la politique	3483
Document de politique JSON	3483
En savoir plus	3483
AWSQuickSightOpenSearchPolicy	3484
Utilisation de cette politique	3484
Détails de la politique	3484
Version de la politique	3484
Document de politique JSON	3484
En savoir plus	3485
AWSQuickSightSageMakerPolicy	3486
Utilisation de cette politique	3486
Détails de la politique	3486
Version de la politique	3486
Document de politique JSON	3486
En savoir plus	3487
AWSQuickSightSecretsManagerWriteAccess	3488
Utilisation de cette politique	3488
Détails de la politique	3488
Version de la politique	3488
Document de politique JSON	3488
En savoir plus	3489

AWSQuickSightSecretsManagerWritePolicy	3489
Utilisation de cette politique	3490
Détails de la politique	3490
Version de la politique	3490
Document de politique JSON	3490
En savoir plus	3491
AWSQuickSightTimestreamPolicy	3491
Utilisation de cette politique	3491
Détails de la politique	3491
Version de la politique	3492
Document de politique JSON	3492
En savoir plus	3492
AWSReachabilityAnalyzerServiceRolePolicy	3493
Utilisation de cette politique	3493
Détails de la politique	3493
Version de la politique	3493
Document de politique JSON	3493
En savoir plus	3496
AWSRefactoringToolkitFullAccess	3496
Utilisation de cette politique	3496
Détails de la politique	3496
Version de la politique	3496
Document de politique JSON	3497
En savoir plus	3510
AWSRefactoringToolkitSidecarPolicy	3510
Utilisation de cette politique	3511
Détails de la politique	3511
Version de la politique	3511
Document de politique JSON	3511
En savoir plus	3512
AWSrePostPrivateCloudWatchAccess	3512
Utilisation de cette politique	3512
Détails de la politique	3513
Version de la politique	3513
Document de politique JSON	3513
En savoir plus	3514

AWSRepostSpaceSupportOperationsPolicy	3514
Utilisation de cette politique	3514
Détails de la politique	3514
Version de la politique	3514
Document de politique JSON	3514
En savoir plus	3515
AWSResilienceHubAssessmentExecutionPolicy	3515
Utilisation de cette politique	3515
Détails de la politique	3515
Version de la politique	3516
Document de politique JSON	3516
En savoir plus	3521
AWSResilienceHubResilienceTestingPolicy	3521
Utilisation de cette politique	3521
Détails de la politique	3521
Version de la politique	3521
Document de politique JSON	3521
En savoir plus	3524
AWSResilienceHubServiceRolePolicy	3525
Utilisation de cette politique	3525
Détails de la politique	3525
Version de la politique	3525
Document de politique JSON	3525
En savoir plus	3526
AWSResilienceHubV2AssessmentExecutionPolicy	3526
Utilisation de cette politique	3526
Détails de la politique	3526
Version de la politique	3527
Document de politique JSON	3527
En savoir plus	3533
AWSResourceAccessManagerFullAccess	3533
Utilisation de cette politique	3533
Détails de la politique	3533
Version de la politique	3533
Document de politique JSON	3534
En savoir plus	3534

AWSResourceAccessManagerReadOnlyAccess	3534
Utilisation de cette politique	3534
Détails de la politique	3534
Version de la politique	3535
Document de politique JSON	3535
En savoir plus	3535
AWSResourceAccessManagerResourceShareParticipantAccess	3535
Utilisation de cette politique	3536
Détails de la politique	3536
Version de la politique	3536
Document de politique JSON	3536
En savoir plus	3537
AWSResourceAccessManagerServiceRolePolicy	3537
Utilisation de cette politique	3537
Détails de la politique	3537
Version de la politique	3537
Document de politique JSON	3538
En savoir plus	3538
AWSResourceExplorerFullAccess	3539
Utilisation de cette politique	3539
Détails de la politique	3539
Version de la politique	3539
Document de politique JSON	3539
En savoir plus	3540
AWSResourceExplorerOrganizationsAccess	3540
Utilisation de cette politique	3541
Détails de la politique	3541
Version de la politique	3541
Document de politique JSON	3541
En savoir plus	3543
AWSResourceExplorerReadOnlyAccess	3543
Utilisation de cette politique	3543
Détails de la politique	3543
Version de la politique	3543
Document de politique JSON	3544
En savoir plus	3544

AWSResourceExplorerServiceRolePolicy	3544
Utilisation de cette politique	3545
Détails de la politique	3545
Version de la politique	3545
Document de politique JSON	3545
En savoir plus	3611
AWSResourceGroupsReadOnlyAccess	3611
Utilisation de cette politique	3611
Détails de la politique	3611
Version de la politique	3612
Document de politique JSON	3612
En savoir plus	3613
AWSRevenueAttributionManagement	3613
Utilisation de cette politique	3614
Détails de la politique	3614
Version de la politique	3614
Document de politique JSON	3614
En savoir plus	3616
AWSRoboMaker_FullAccess	3616
Utilisation de cette politique	3616
Détails de la politique	3616
Version de la politique	3617
Document de politique JSON	3617
En savoir plus	3618
AWSRoboMakerReadOnlyAccess	3618
Utilisation de cette politique	3618
Détails de la politique	3618
Version de la politique	3619
Document de politique JSON	3619
En savoir plus	3619
AWSRoboMakerServicePolicy	3620
Utilisation de cette politique	3620
Détails de la politique	3620
Version de la politique	3620
Document de politique JSON	3620
En savoir plus	3622

AWSRoboMakerServiceRolePolicy	3622
Utilisation de cette politique	3622
Détails de la politique	3622
Version de la politique	3622
Document de politique JSON	3623
En savoir plus	3624
AWSRolesAnywhereFullAccess	3624
Utilisation de cette politique	3624
Détails de la politique	3624
Version de la politique	3624
Document de politique JSON	3625
En savoir plus	3627
AWSRolesAnywhereReadOnly	3627
Utilisation de cette politique	3627
Détails de la politique	3628
Version de la politique	3628
Document de politique JSON	3628
En savoir plus	3629
AWSRolesAnywhereServicePolicy	3630
Utilisation de cette politique	3630
Détails de la politique	3630
Version de la politique	3630
Document de politique JSON	3630
En savoir plus	3631
AWSS3OnOutpostsServiceRolePolicy	3631
Utilisation de cette politique	3631
Détails de la politique	3632
Version de la politique	3632
Document de politique JSON	3632
En savoir plus	3635
AWSSavingsPlansFullAccess	3635
Utilisation de cette politique	3635
Détails de la politique	3635
Version de la politique	3635
Document de politique JSON	3635
En savoir plus	3636

AWSSavingsPlansReadOnlyAccess	3636
Utilisation de cette politique	3636
Détails de la politique	3636
Version de la politique	3636
Document de politique JSON	3637
En savoir plus	3637
AWSSDMPServiceRolePolicy	3637
Utilisation de cette politique	3637
Détails de la politique	3637
Version de la politique	3638
Document de politique JSON	3638
En savoir plus	3641
AWS SecretsManagerClientReadOnlyAccess	3641
Utilisation de cette politique	3641
Détails de la politique	3641
Version de la politique	3642
Document de politique JSON	3642
En savoir plus	3643
AWS SecurityAgentServiceRolePolicy	3643
Utilisation de cette politique	3643
Détails de la politique	3643
Version de la politique	3643
Document de politique JSON	3644
En savoir plus	3646
AWS SecurityAgentWebAppPolicy	3646
Utilisation de cette politique	3646
Détails de la politique	3646
Version de la politique	3646
Document de politique JSON	3646
En savoir plus	3649
AWS SecurityHubFullAccess	3649
Utilisation de cette politique	3649
Détails de la politique	3649
Version de la politique	3649
Document de politique JSON	3650
En savoir plus	3651

AWSSecurityHubOrganizationsAccess	3651
Utilisation de cette politique	3651
Détails de la politique	3651
Version de la politique	3652
Document de politique JSON	3652
En savoir plus	3654
AWSSecurityHubReadOnlyAccess	3655
Utilisation de cette politique	3655
Détails de la politique	3655
Version de la politique	3655
Document de politique JSON	3655
En savoir plus	3656
AWSSecurityHubServiceRolePolicy	3656
Utilisation de cette politique	3656
Détails de la politique	3656
Version de la politique	3656
Document de politique JSON	3657
En savoir plus	3660
AWSSecurityHubV2ServiceRolePolicy	3660
Utilisation de cette politique	3660
Détails de la politique	3660
Version de la politique	3660
Document de politique JSON	3660
En savoir plus	3666
AWSSecurityIncidentResponseCaseFullAccess	3667
Utilisation de cette politique	3667
Détails de la politique	3667
Version de la politique	3667
Document de politique JSON	3667
En savoir plus	3668
AWSSecurityIncidentResponseFullAccess	3668
Utilisation de cette politique	3669
Détails de la politique	3669
Version de la politique	3669
Document de politique JSON	3669
En savoir plus	3671

AWSSecurityIncidentResponseReadOnlyAccess	3671
Utilisation de cette politique	3671
Détails de la politique	3671
Version de la politique	3671
Document de politique JSON	3672
En savoir plus	3672
AWSSecurityIncidentResponseServiceRolePolicy	3672
Utilisation de cette politique	3673
Détails de la politique	3673
Version de la politique	3673
Document de politique JSON	3673
En savoir plus	3674
AWSSecurityIncidentResponseTriageServiceRolePolicy	3675
Utilisation de cette politique	3675
Détails de la politique	3675
Version de la politique	3675
Document de politique JSON	3675
En savoir plus	3678
AWSServiceCatalogAdminFullAccess	3678
Utilisation de cette politique	3678
Détails de la politique	3678
Version de la politique	3678
Document de politique JSON	3678
En savoir plus	3681
AWSServiceCatalogAdminReadOnlyAccess	3681
Utilisation de cette politique	3682
Détails de la politique	3682
Version de la politique	3682
Document de politique JSON	3682
En savoir plus	3683
AWSServiceCatalogAppRegistryFullAccess	3684
Utilisation de cette politique	3684
Détails de la politique	3684
Version de la politique	3684
Document de politique JSON	3684
En savoir plus	3687

AWSServiceCatalogAppRegistryReadOnlyAccess	3687
Utilisation de cette politique	3687
Détails de la politique	3687
Version de la politique	3688
Document de politique JSON	3688
En savoir plus	3688
AWSServiceCatalogAppRegistryServiceRolePolicy	3689
Utilisation de cette politique	3689
Détails de la politique	3689
Version de la politique	3689
Document de politique JSON	3689
En savoir plus	3691
AWSServiceCatalogEndUserFullAccess	3691
Utilisation de cette politique	3691
Détails de la politique	3691
Version de la politique	3691
Document de politique JSON	3691
En savoir plus	3693
AWSServiceCatalogEndUserReadOnlyAccess	3694
Utilisation de cette politique	3694
Détails de la politique	3694
Version de la politique	3694
Document de politique JSON	3694
En savoir plus	3696
AWSServiceCatalogOrgsDataSyncServiceRolePolicy	3696
Utilisation de cette politique	3696
Détails de la politique	3696
Version de la politique	3697
Document de politique JSON	3697
En savoir plus	3698
AWSServiceCatalogSyncServiceRolePolicy	3698
Utilisation de cette politique	3698
Détails de la politique	3698
Version de la politique	3698
Document de politique JSON	3699
En savoir plus	3700

AWSServiceRoleForAIDevOpsPolicy	3700
Utilisation de cette politique	3700
Détails de la politique	3700
Version de la politique	3700
Document de politique JSON	3700
En savoir plus	3703
AWSServiceRoleForAmazonEKSNodegroup	3703
Utilisation de cette politique	3703
Détails de la politique	3703
Version de la politique	3703
Document de politique JSON	3704
En savoir plus	3709
AWSServiceRoleForAmazonQDeveloper	3709
Utilisation de cette politique	3709
Détails de la politique	3710
Version de la politique	3710
Document de politique JSON	3710
En savoir plus	3711
AWSServiceRoleForAWSTransform	3711
Utilisation de cette politique	3711
Détails de la politique	3711
Version de la politique	3711
Document de politique JSON	3712
En savoir plus	3714
AWSServiceRoleForAWSTransformCustom	3714
Utilisation de cette politique	3714
Détails de la politique	3714
Version de la politique	3715
Document de politique JSON	3715
En savoir plus	3716
AWSServiceRoleForCloudWatchAlarmsActionSSMSERVICERolePolicy	3716
Utilisation de cette politique	3716
Détails de la politique	3716
Version de la politique	3716
Document de politique JSON	3717
En savoir plus	3717

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy	3717
Utilisation de cette politique	3717
Détails de la politique	3717
Version de la politique	3718
Document de politique JSON	3718
En savoir plus	3718
AWSServiceRoleForCodeGuru-Profiler	3719
Utilisation de cette politique	3719
Détails de la politique	3719
Version de la politique	3719
Document de politique JSON	3719
En savoir plus	3720
AWSServiceRoleForCodeWhispererPolicy	3720
Utilisation de cette politique	3720
Détails de la politique	3720
Version de la politique	3720
Document de politique JSON	3721
En savoir plus	3723
AWSServiceRoleForEC2ScheduledInstances	3723
Utilisation de cette politique	3723
Détails de la politique	3724
Version de la politique	3724
Document de politique JSON	3724
En savoir plus	3725
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy	3725
Utilisation de cette politique	3725
Détails de la politique	3725
Version de la politique	3726
Document de politique JSON	3726
En savoir plus	3726
AWSServiceRoleForImageBuilder	3726
Utilisation de cette politique	3726
Détails de la politique	3727
Version de la politique	3727
Document de politique JSON	3727
En savoir plus	3738

AWSServiceRoleForIoTSiteWise	3738
Utilisation de cette politique	3738
Détails de la politique	3739
Version de la politique	3739
Document de politique JSON	3739
En savoir plus	3740
AWSServiceRoleForLogDeliveryPolicy	3740
Utilisation de cette politique	3741
Détails de la politique	3741
Version de la politique	3741
Document de politique JSON	3741
En savoir plus	3742
AWSServiceRoleForMonitronPolicy	3742
Utilisation de cette politique	3742
Détails de la politique	3742
Version de la politique	3743
Document de politique JSON	3743
En savoir plus	3744
AWSServiceRoleForNeptuneGraphPolicy	3744
Utilisation de cette politique	3745
Détails de la politique	3745
Version de la politique	3745
Document de politique JSON	3745
En savoir plus	3746
AWSServiceRoleForPrivateMarketplaceAdminPolicy	3747
Utilisation de cette politique	3747
Détails de la politique	3747
Version de la politique	3747
Document de politique JSON	3747
En savoir plus	3749
AWSServiceRoleForProcurementInsightsPolicy	3749
Utilisation de cette politique	3749
Détails de la politique	3749
Version de la politique	3750
Document de politique JSON	3750
En savoir plus	3750

AWSServiceRoleForSMS	3750
Utilisation de cette politique	3751
Détails de la politique	3751
Version de la politique	3751
Document de politique JSON	3751
En savoir plus	3758
AWSServiceRoleForUserSubscriptions	3758
Utilisation de cette politique	3758
Détails de la politique	3758
Version de la politique	3758
Document de politique JSON	3759
En savoir plus	3760
AWSServiceRolePolicyForBackupReports	3760
Utilisation de cette politique	3760
Détails de la politique	3760
Version de la politique	3761
Document de politique JSON	3761
En savoir plus	3762
AWSServiceRolePolicyForBackupRestoreTesting	3762
Utilisation de cette politique	3762
Détails de la politique	3763
Version de la politique	3763
Document de politique JSON	3763
En savoir plus	3766
AWSServiceRolePolicyForWorkspacesInstances	3766
Utilisation de cette politique	3766
Détails de la politique	3766
Version de la politique	3766
Document de politique JSON	3767
En savoir plus	3768
AWSShieldDRTAccessPolicy	3769
Utilisation de cette politique	3769
Détails de la politique	3769
Version de la politique	3769
Document de politique JSON	3769
En savoir plus	3770

AWSShieldServiceRolePolicy	3770
Utilisation de cette politique	3771
Détails de la politique	3771
Version de la politique	3771
Document de politique JSON	3771
En savoir plus	3772
AWSSocialMessagingServiceRolePolicy	3772
Utilisation de cette politique	3772
Détails de la politique	3772
Version de la politique	3772
Document de politique JSON	3772
En savoir plus	3773
AWSSSMForSAPServiceLinkedRolePolicy	3773
Utilisation de cette politique	3773
Détails de la politique	3773
Version de la politique	3774
Document de politique JSON	3774
En savoir plus	3782
AWSSSMOpsInsightsServiceRolePolicy	3782
Utilisation de cette politique	3783
Détails de la politique	3783
Version de la politique	3783
Document de politique JSON	3783
En savoir plus	3784
AWSSSODirectoryAdministrator	3784
Utilisation de cette politique	3784
Détails de la politique	3784
Version de la politique	3784
Document de politique JSON	3785
En savoir plus	3785
AWSSSODirectoryReadOnly	3786
Utilisation de cette politique	3786
Détails de la politique	3786
Version de la politique	3786
Document de politique JSON	3786
En savoir plus	3787

AWSSSOMasterAccountAdministrator	3787
Utilisation de cette politique	3788
Détails de la politique	3788
Version de la politique	3788
Document de politique JSON	3788
En savoir plus	3791
AWSSSOMemberAccountAdministrator	3791
Utilisation de cette politique	3791
Détails de la politique	3791
Version de la politique	3792
Document de politique JSON	3792
En savoir plus	3794
AWSSSOReadOnly	3794
Utilisation de cette politique	3794
Détails de la politique	3794
Version de la politique	3795
Document de politique JSON	3795
En savoir plus	3796
AWSSSOServiceRolePolicy	3796
Utilisation de cette politique	3797
Détails de la politique	3797
Version de la politique	3797
Document de politique JSON	3797
En savoir plus	3801
AWSSStepFunctionsConsoleFullAccess	3801
Utilisation de cette politique	3801
Détails de la politique	3801
Version de la politique	3801
Document de politique JSON	3802
En savoir plus	3802
AWSSStepFunctionsFullAccess	3803
Utilisation de cette politique	3803
Détails de la politique	3803
Version de la politique	3803
Document de politique JSON	3803
En savoir plus	3804

AWSStepFunctionsReadOnlyAccess	3804
Utilisation de cette politique	3804
Détails de la politique	3804
Version de la politique	3804
Document de politique JSON	3805
En savoir plus	3805
AWSSStorageGatewayFullAccess	3805
Utilisation de cette politique	3806
Détails de la politique	3806
Version de la politique	3806
Document de politique JSON	3806
En savoir plus	3807
AWSSStorageGatewayReadOnlyAccess	3807
Utilisation de cette politique	3807
Détails de la politique	3807
Version de la politique	3807
Document de politique JSON	3808
En savoir plus	3808
AWSSStorageGatewayServiceRolePolicy	3809
Utilisation de cette politique	3809
Détails de la politique	3809
Version de la politique	3809
Document de politique JSON	3809
En savoir plus	3810
AWSSupplyChainFederationAdminAccess	3810
Utilisation de cette politique	3810
Détails de la politique	3810
Version de la politique	3810
Document de politique JSON	3811
En savoir plus	3817
AWSSupportAccess	3818
Utilisation de cette politique	3818
Détails de la politique	3818
Version de la politique	3818
Document de politique JSON	3818
En savoir plus	3819

AWSSupportAppFullAccess	3819
Utilisation de cette politique	3819
Détails de la politique	3819
Version de la politique	3819
Document de politique JSON	3820
En savoir plus	3820
AWSSupportAppReadOnlyAccess	3821
Utilisation de cette politique	3821
Détails de la politique	3821
Version de la politique	3821
Document de politique JSON	3821
En savoir plus	3822
AWSSupportPlansFullAccess	3822
Utilisation de cette politique	3822
Détails de la politique	3822
Version de la politique	3822
Document de politique JSON	3822
En savoir plus	3823
AWSSupportPlansReadOnlyAccess	3824
Utilisation de cette politique	3824
Détails de la politique	3824
Version de la politique	3824
Document de politique JSON	3824
En savoir plus	3825
AWSSupportPlansServiceRolePolicy	3825
Utilisation de cette politique	3825
Détails de la politique	3825
Version de la politique	3826
Document de politique JSON	3826
En savoir plus	3826
AWSSupportServiceRolePolicy	3827
Utilisation de cette politique	3827
Détails de la politique	3827
Version de la politique	3827
Document de politique JSON	3827
En savoir plus	3933

AWSSystemsManagerAccountDiscoveryServicePolicy	3933
Utilisation de cette politique	3933
Détails de la politique	3933
Version de la politique	3933
Document de politique JSON	3934
En savoir plus	3934
AWSSystemsManagerChangeManagementServicePolicy	3934
Utilisation de cette politique	3934
Détails de la politique	3935
Version de la politique	3935
Document de politique JSON	3935
En savoir plus	3937
AWSSystemsManagerEnableConfigRecordingExecutionPolicy	3938
Utilisation de cette politique	3938
Détails de la politique	3938
Version de la politique	3938
Document de politique JSON	3938
En savoir plus	3940
AWSSystemsManagerEnableExplorerExecutionPolicy	3940
Utilisation de cette politique	3941
Détails de la politique	3941
Version de la politique	3941
Document de politique JSON	3941
En savoir plus	3942
AWSSystemsManagerForSAPFullAccess	3943
Utilisation de cette politique	3943
Détails de la politique	3943
Version de la politique	3943
Document de politique JSON	3943
En savoir plus	3944
AWSSystemsManagerForSAPReadOnlyAccess	3945
Utilisation de cette politique	3945
Détails de la politique	3945
Version de la politique	3945
Document de politique JSON	3945
En savoir plus	3946

AWSSystemsManagerJustInTimeAccessServicePolicy	3946
Utilisation de cette politique	3946
Détails de la politique	3946
Version de la politique	3946
Document de politique JSON	3947
En savoir plus	3952
AWSSystemsManagerJustInTimeAccessTokenPolicy	3952
Utilisation de cette politique	3952
Détails de la politique	3952
Version de la politique	3953
Document de politique JSON	3953
En savoir plus	3956
AWSSystemsManagerJustInTimeAccessTokenSessionPolicy	3956
Utilisation de cette politique	3956
Détails de la politique	3956
Version de la politique	3956
Document de politique JSON	3957
En savoir plus	3959
AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy	3959
Utilisation de cette politique	3959
Détails de la politique	3960
Version de la politique	3960
Document de politique JSON	3960
En savoir plus	3964
AWSSystemsManagerNotificationsServicePolicy	3964
Utilisation de cette politique	3965
Détails de la politique	3965
Version de la politique	3965
Document de politique JSON	3965
En savoir plus	3966
AWSSystemsManagerOpsDataSyncServiceRolePolicy	3967
Utilisation de cette politique	3967
Détails de la politique	3967
Version de la politique	3967
Document de politique JSON	3967
En savoir plus	3971

AWSThinkboxAssetServerPolicy	3971
Utilisation de cette politique	3971
Détails de la politique	3971
Version de la politique	3971
Document de politique JSON	3972
En savoir plus	3972
AWSThinkboxAWSPortalAdminPolicy	3973
Utilisation de cette politique	3973
Détails de la politique	3973
Version de la politique	3973
Document de politique JSON	3973
En savoir plus	3983
AWSThinkboxAWSPortalGatewayPolicy	3983
Utilisation de cette politique	3983
Détails de la politique	3984
Version de la politique	3984
Document de politique JSON	3984
En savoir plus	3986
AWSThinkboxAWSPortalWorkerPolicy	3986
Utilisation de cette politique	3986
Détails de la politique	3986
Version de la politique	3986
Document de politique JSON	3987
En savoir plus	3988
AWSThinkboxDeadlineResourceTrackerAccessPolicy	3989
Utilisation de cette politique	3989
Détails de la politique	3989
Version de la politique	3989
Document de politique JSON	3989
En savoir plus	3992
AWSThinkboxDeadlineResourceTrackerAdminPolicy	3992
Utilisation de cette politique	3992
Détails de la politique	3993
Version de la politique	3993
Document de politique JSON	3993
En savoir plus	3999

AWSThinkboxDeadlineSpotEventPluginAdminPolicy	3999
Utilisation de cette politique	3999
Détails de la politique	3999
Version de la politique	4000
Document de politique JSON	4000
En savoir plus	4002
AWSThinkboxDeadlineSpotEventPluginWorkerPolicy	4003
Utilisation de cette politique	4003
Détails de la politique	4003
Version de la politique	4003
Document de politique JSON	4003
En savoir plus	4005
AWSTransferConsoleFullAccess	4005
Utilisation de cette politique	4005
Détails de la politique	4005
Version de la politique	4005
Document de politique JSON	4006
En savoir plus	4006
AWSTransferFullAccess	4007
Utilisation de cette politique	4007
Détails de la politique	4007
Version de la politique	4007
Document de politique JSON	4007
En savoir plus	4008
AWSTransferLoggingAccess	4008
Utilisation de cette politique	4008
Détails de la politique	4009
Version de la politique	4009
Document de politique JSON	4009
En savoir plus	4009
AWSTransferReadOnlyAccess	4010
Utilisation de cette politique	4010
Détails de la politique	4010
Version de la politique	4010
Document de politique JSON	4010
En savoir plus	4011

AWSTransferServiceRolePolicy	4011
Utilisation de cette politique	4011
Détails de la politique	4011
Version de la politique	4011
Document de politique JSON	4012
En savoir plus	4013
AWSTransformApplicationDeploymentPolicy	4013
Utilisation de cette politique	4013
Détails de la politique	4014
Version de la politique	4014
Document de politique JSON	4014
En savoir plus	4022
AWSTransformApplicationECSDeploymentPolicy	4023
Utilisation de cette politique	4023
Détails de la politique	4023
Version de la politique	4023
Document de politique JSON	4023
En savoir plus	4032
AWSTransformCustomExecuteTransformations	4032
Utilisation de cette politique	4032
Détails de la politique	4032
Version de la politique	4032
Document de politique JSON	4032
En savoir plus	4033
AWSTransformCustomFullAccess	4034
Utilisation de cette politique	4034
Détails de la politique	4034
Version de la politique	4034
Document de politique JSON	4034
En savoir plus	4035
AWSTransformCustomManageTransformations	4035
Utilisation de cette politique	4035
Détails de la politique	4036
Version de la politique	4036
Document de politique JSON	4036
En savoir plus	4037

AWSTransformInfrastructureExecutorAccessBatch	4037
Utilisation de cette politique	4038
Détails de la politique	4038
Version de la politique	4038
Document de politique JSON	4038
En savoir plus	4045
AWSTransformInfrastructureExecutorAccessEC2	4045
Utilisation de cette politique	4045
Détails de la politique	4046
Version de la politique	4046
Document de politique JSON	4046
En savoir plus	4053
AWSTransformLandingZoneAgentPolicy	4053
Utilisation de cette politique	4054
Détails de la politique	4054
Version de la politique	4054
Document de politique JSON	4054
En savoir plus	4062
AWSTransformNetworkMigrationAgentPolicy	4062
Utilisation de cette politique	4062
Détails de la politique	4062
Version de la politique	4063
Document de politique JSON	4063
En savoir plus	4091
AWSTransformRevenueAttributionPolicy	4091
Utilisation de cette politique	4091
Détails de la politique	4091
Version de la politique	4091
Document de politique JSON	4092
En savoir plus	4092
AWSTransformSecretsManagerConnectorPolicy	4092
Utilisation de cette politique	4093
Détails de la politique	4093
Version de la politique	4093
Document de politique JSON	4093
En savoir plus	4094

AWSTransformSecurityAgentExecutorAccess	4095
Utilisation de cette politique	4095
Détails de la politique	4095
Version de la politique	4095
Document de politique JSON	4095
En savoir plus	4097
AWSTransformServerMigrationAgentPolicy	4098
Utilisation de cette politique	4098
Détails de la politique	4098
Version de la politique	4098
Document de politique JSON	4098
En savoir plus	4122
AWSTrustedAdvisorPriorityFullAccess	4122
Utilisation de cette politique	4123
Détails de la politique	4123
Version de la politique	4123
Document de politique JSON	4123
En savoir plus	4125
AWSTrustedAdvisorPriorityReadOnlyAccess	4125
Utilisation de cette politique	4125
Détails de la politique	4125
Version de la politique	4126
Document de politique JSON	4126
En savoir plus	4127
AWSTrustedAdvisorReportingServiceRolePolicy	4127
Utilisation de cette politique	4127
Détails de la politique	4127
Version de la politique	4127
Document de politique JSON	4128
En savoir plus	4128
AWSTrustedAdvisorServiceRolePolicy	4128
Utilisation de cette politique	4129
Détails de la politique	4129
Version de la politique	4129
Document de politique JSON	4129
En savoir plus	4132

AWSUserAttributeCostAllocationPolicy	4132
Utilisation de cette politique	4132
Détails de la politique	4133
Version de la politique	4133
Document de politique JSON	4133
En savoir plus	4133
AWSUserNotificationsServiceLinkedRolePolicy	4134
Utilisation de cette politique	4134
Détails de la politique	4134
Version de la politique	4134
Document de politique JSON	4134
En savoir plus	4136
AWSVendorInsightsAssessorFullAccess	4136
Utilisation de cette politique	4136
Détails de la politique	4136
Version de la politique	4137
Document de politique JSON	4137
En savoir plus	4138
AWSVendorInsightsAssessorReadOnly	4138
Utilisation de cette politique	4138
Détails de la politique	4138
Version de la politique	4139
Document de politique JSON	4139
En savoir plus	4139
AWSVendorInsightsVendorFullAccess	4140
Utilisation de cette politique	4140
Détails de la politique	4140
Version de la politique	4140
Document de politique JSON	4140
En savoir plus	4142
AWSVendorInsightsVendorReadOnly	4142
Utilisation de cette politique	4142
Détails de la politique	4142
Version de la politique	4143
Document de politique JSON	4143
En savoir plus	4144

AWSVPCFlowLogsServiceRolePolicy	4144
Utilisation de cette politique	4144
Détails de la politique	4144
Version de la politique	4144
Document de politique JSON	4145
En savoir plus	4146
AWSVpcLatticeServiceRolePolicy	4146
Utilisation de cette politique	4146
Détails de la politique	4147
Version de la politique	4147
Document de politique JSON	4147
En savoir plus	4150
AWSVPCS2SVpnServiceRolePolicy	4150
Utilisation de cette politique	4150
Détails de la politique	4150
Version de la politique	4150
Document de politique JSON	4150
En savoir plus	4152
AWSVPCTransitGatewayServiceRolePolicy	4152
Utilisation de cette politique	4152
Détails de la politique	4152
Version de la politique	4152
Document de politique JSON	4152
En savoir plus	4153
AWSVPCVerifiedAccessServiceRolePolicy	4153
Utilisation de cette politique	4153
Détails de la politique	4153
Version de la politique	4154
Document de politique JSON	4154
En savoir plus	4155
AWSWAFConsoleFullAccess	4156
Utilisation de cette politique	4156
Détails de la politique	4156
Version de la politique	4156
Document de politique JSON	4156
En savoir plus	4165

AWSWAFAConsoleReadOnlyAccess	4166
Utilisation de cette politique	4166
Détails de la politique	4166
Version de la politique	4166
Document de politique JSON	4166
En savoir plus	4174
AWSWAFFullAccess	4174
Utilisation de cette politique	4174
Détails de la politique	4174
Version de la politique	4175
Document de politique JSON	4175
En savoir plus	4181
AWSWAFReadOnlyAccess	4181
Utilisation de cette politique	4181
Détails de la politique	4181
Version de la politique	4181
Document de politique JSON	4181
En savoir plus	4186
AWSWellArchitectedAgentOrganizationsServiceRolePolicy	4186
Utilisation de cette politique	4186
Détails de la politique	4186
Version de la politique	4186
Document de politique JSON	4187
En savoir plus	4187
AWSWellArchitectedAgentResourceScanningServiceRolePolicy	4187
Utilisation de cette politique	4188
Détails de la politique	4188
Version de la politique	4188
Document de politique JSON	4188
En savoir plus	4252
AWSWellArchitectedDiscoveryServiceRolePolicy	4253
Utilisation de cette politique	4253
Détails de la politique	4253
Version de la politique	4253
Document de politique JSON	4253
En savoir plus	4255

AWSWellArchitectedOrganizationsServiceRolePolicy	4255
Utilisation de cette politique	4255
Détails de la politique	4255
Version de la politique	4255
Document de politique JSON	4256
En savoir plus	4256
AWSWickrFullAccess	4256
Utilisation de cette politique	4256
Détails de la politique	4257
Version de la politique	4257
Document de politique JSON	4257
En savoir plus	4257
AWSXrayCrossAccountSharingConfiguration	4258
Utilisation de cette politique	4258
Détails de la politique	4258
Version de la politique	4258
Document de politique JSON	4258
En savoir plus	4259
AWSXRayDaemonWriteAccess	4259
Utilisation de cette politique	4260
Détails de la politique	4260
Version de la politique	4260
Document de politique JSON	4260
En savoir plus	4261
AWSXrayFullAccess	4261
Utilisation de cette politique	4261
Détails de la politique	4261
Version de la politique	4261
Document de politique JSON	4261
En savoir plus	4262
AWSXrayReadOnlyAccess	4262
Utilisation de cette politique	4262
Détails de la politique	4262
Version de la politique	4263
Document de politique JSON	4263
En savoir plus	4264

AWSXrayWriteOnlyAccess	4264
Utilisation de cette politique	4264
Détails de la politique	4264
Version de la politique	4264
Document de politique JSON	4264
En savoir plus	4265
AWSZonalAutoshiftPracticeRunSLRPolicy	4265
Utilisation de cette politique	4265
Détails de la politique	4265
Version de la politique	4266
Document de politique JSON	4266
En savoir plus	4267
AWSZoneGroupAccessManagementServiceRolePolicy	4267
Utilisation de cette politique	4267
Détails de la politique	4267
Version de la politique	4267
Document de politique JSON	4268
En savoir plus	4268
BatchServiceRolePolicy	4268
Utilisation de cette politique	4269
Détails de la politique	4269
Version de la politique	4269
Document de politique JSON	4269
En savoir plus	4276
BedrockAgentCoreFullAccess	4276
Utilisation de cette politique	4276
Détails de la politique	4276
Version de la politique	4276
Document de politique JSON	4277
En savoir plus	4288
BedrockAgentCoreNetworkServiceRolePolicy	4288
Utilisation de cette politique	4288
Détails de la politique	4288
Version de la politique	4289
Document de politique JSON	4289
En savoir plus	4291

BedrockAgentCoreRuntimeIdentityServiceRolePolicy	4291
Utilisation de cette politique	4291
Détails de la politique	4291
Version de la politique	4291
Document de politique JSON	4292
En savoir plus	4292
BedrockAgentCoreRuntimeInstancesInstanceRolePolicy	4292
Utilisation de cette politique	4292
Détails de la politique	4292
Version de la politique	4293
Document de politique JSON	4293
En savoir plus	4293
BedrockAgentCoreRuntimeInstancesOperatorRolePolicy	4294
Utilisation de cette politique	4294
Détails de la politique	4294
Version de la politique	4294
Document de politique JSON	4294
En savoir plus	4301
Billing	4302
Utilisation de cette politique	4302
Détails de la politique	4302
Version de la politique	4302
Document de politique JSON	4302
En savoir plus	4306
BudgetsServiceRolePolicy	4306
Utilisation de cette politique	4307
Détails de la politique	4307
Version de la politique	4307
Document de politique JSON	4307
En savoir plus	4307
CertificateManagerServiceRolePolicy	4308
Utilisation de cette politique	4308
Détails de la politique	4308
Version de la politique	4308
Document de politique JSON	4308
En savoir plus	4309

ClientVPNServiceConnectionsRolePolicy	4309
Utilisation de cette politique	4309
Détails de la politique	4309
Version de la politique	4309
Document de politique JSON	4310
En savoir plus	4310
ClientVPNServiceRolePolicy	4310
Utilisation de cette politique	4310
Détails de la politique	4310
Version de la politique	4311
Document de politique JSON	4311
En savoir plus	4312
CloudFormationStackSetsOrgAdminServiceRolePolicy	4312
Utilisation de cette politique	4312
Détails de la politique	4312
Version de la politique	4312
Document de politique JSON	4312
En savoir plus	4313
CloudFormationStackSetsOrgMemberServiceRolePolicy	4313
Utilisation de cette politique	4313
Détails de la politique	4313
Version de la politique	4314
Document de politique JSON	4314
En savoir plus	4315
CloudFrontFullAccess	4315
Utilisation de cette politique	4316
Détails de la politique	4316
Version de la politique	4316
Document de politique JSON	4316
En savoir plus	4318
CloudFrontReadOnlyAccess	4318
Utilisation de cette politique	4318
Détails de la politique	4319
Version de la politique	4319
Document de politique JSON	4319
En savoir plus	4320

CloudHSMServiceRolePolicy	4320
Utilisation de cette politique	4320
Détails de la politique	4320
Version de la politique	4320
Document de politique JSON	4321
En savoir plus	4321
CloudSearchFullAccess	4321
Utilisation de cette politique	4321
Détails de la politique	4322
Version de la politique	4322
Document de politique JSON	4322
En savoir plus	4322
CloudSearchReadOnlyAccess	4323
Utilisation de cette politique	4323
Détails de la politique	4323
Version de la politique	4323
Document de politique JSON	4323
En savoir plus	4324
CloudTrailEventContext	4324
Utilisation de cette politique	4324
Détails de la politique	4324
Version de la politique	4324
Document de politique JSON	4325
En savoir plus	4326
CloudTrailServiceRolePolicy	4326
Utilisation de cette politique	4327
Détails de la politique	4327
Version de la politique	4327
Document de politique JSON	4327
En savoir plus	4329
CloudWatch-CrossAccountAccess	4329
Utilisation de cette politique	4329
Détails de la politique	4329
Version de la politique	4329
Document de politique JSON	4330
En savoir plus	4330

CloudWatchActionsEC2Access	4330
Utilisation de cette politique	4330
Détails de la politique	4330
Version de la politique	4331
Document de politique JSON	4331
En savoir plus	4331
CloudWatchAgentAdminPolicy	4331
Utilisation de cette politique	4332
Détails de la politique	4332
Version de la politique	4332
Document de politique JSON	4332
En savoir plus	4333
CloudWatchAgentServerPolicy	4333
Utilisation de cette politique	4333
Détails de la politique	4333
Version de la politique	4334
Document de politique JSON	4334
En savoir plus	4335
CloudWatchAPIKeyAccess	4335
Utilisation de cette politique	4335
Détails de la politique	4335
Version de la politique	4335
Document de politique JSON	4335
En savoir plus	4336
CloudWatchApplicationInsightsFullAccess	4336
Utilisation de cette politique	4337
Détails de la politique	4337
Version de la politique	4337
Document de politique JSON	4337
En savoir plus	4338
CloudWatchApplicationInsightsReadOnlyAccess	4339
Utilisation de cette politique	4339
Détails de la politique	4339
Version de la politique	4339
Document de politique JSON	4339
En savoir plus	4340

CloudwatchApplicationInsightsServiceLinkedRolePolicy	4340
Utilisation de cette politique	4340
Détails de la politique	4340
Version de la politique	4340
Document de politique JSON	4341
En savoir plus	4351
CloudWatchApplicationSignalsFullAccess	4351
Utilisation de cette politique	4351
Détails de la politique	4352
Version de la politique	4352
Document de politique JSON	4352
En savoir plus	4357
CloudWatchApplicationSignalsReadOnlyAccess	4357
Utilisation de cette politique	4358
Détails de la politique	4358
Version de la politique	4358
Document de politique JSON	4358
En savoir plus	4362
CloudWatchApplicationSignalsServiceRolePolicy	4362
Utilisation de cette politique	4363
Détails de la politique	4363
Version de la politique	4363
Document de politique JSON	4363
En savoir plus	4366
CloudWatchAutomaticDashboardsAccess	4366
Utilisation de cette politique	4366
Détails de la politique	4367
Version de la politique	4367
Document de politique JSON	4367
En savoir plus	4368
CloudWatchCrossAccountSharingConfiguration	4369
Utilisation de cette politique	4369
Détails de la politique	4369
Version de la politique	4369
Document de politique JSON	4369
En savoir plus	4370

CloudWatchEventsBuiltInTargetExecutionAccess	4370
Utilisation de cette politique	4371
Détails de la politique	4371
Version de la politique	4371
Document de politique JSON	4371
En savoir plus	4372
CloudWatchEventsFullAccess	4372
Utilisation de cette politique	4372
Détails de la politique	4372
Version de la politique	4372
Document de politique JSON	4372
En savoir plus	4374
CloudWatchEventsInvocationAccess	4375
Utilisation de cette politique	4375
Détails de la politique	4375
Version de la politique	4375
Document de politique JSON	4375
En savoir plus	4376
CloudWatchEventsReadOnlyAccess	4376
Utilisation de cette politique	4376
Détails de la politique	4376
Version de la politique	4376
Document de politique JSON	4377
En savoir plus	4378
CloudWatchEventsServiceRolePolicy	4378
Utilisation de cette politique	4378
Détails de la politique	4378
Version de la politique	4379
Document de politique JSON	4379
En savoir plus	4379
CloudWatchFullAccess	4379
Utilisation de cette politique	4380
Détails de la politique	4380
Version de la politique	4380
Document de politique JSON	4380
En savoir plus	4381

CloudWatchFullAccessV2	4381
Utilisation de cette politique	4381
Détails de la politique	4382
Version de la politique	4382
Document de politique JSON	4382
En savoir plus	4388
CloudWatchInternetMonitorFullAccess	4388
Utilisation de cette politique	4388
Détails de la politique	4389
Version de la politique	4389
Document de politique JSON	4389
En savoir plus	4391
CloudWatchInternetMonitorReadOnlyAccess	4391
Utilisation de cette politique	4391
Détails de la politique	4391
Version de la politique	4392
Document de politique JSON	4392
En savoir plus	4392
CloudWatchInternetMonitorServiceRolePolicy	4393
Utilisation de cette politique	4393
Détails de la politique	4393
Version de la politique	4393
Document de politique JSON	4393
En savoir plus	4394
CloudWatchLambdaApplicationSignalsExecutionRolePolicy	4395
Utilisation de cette politique	4395
Détails de la politique	4395
Version de la politique	4395
Document de politique JSON	4395
En savoir plus	4396
CloudWatchLambdaInsightsExecutionRolePolicy	4396
Utilisation de cette politique	4397
Détails de la politique	4397
Version de la politique	4397
Document de politique JSON	4397
En savoir plus	4398

CloudWatchLogsAPIKeyAccess	4398
Utilisation de cette politique	4398
Détails de la politique	4398
Version de la politique	4398
Document de politique JSON	4399
En savoir plus	4400
CloudWatchLogsCrossAccountSharingConfiguration	4400
Utilisation de cette politique	4400
Détails de la politique	4400
Version de la politique	4400
Document de politique JSON	4401
En savoir plus	4402
CloudWatchLogsFullAccess	4402
Utilisation de cette politique	4402
Détails de la politique	4402
Version de la politique	4402
Document de politique JSON	4402
En savoir plus	4403
CloudWatchLogsReadOnlyAccess	4403
Utilisation de cette politique	4403
Détails de la politique	4403
Version de la politique	4404
Document de politique JSON	4404
En savoir plus	4404
CloudWatchNetworkFlowMonitorAgentPublishPolicy	4405
Utilisation de cette politique	4405
Détails de la politique	4405
Version de la politique	4405
Document de politique JSON	4405
En savoir plus	4406
CloudWatchNetworkFlowMonitorServiceRolePolicy	4406
Utilisation de cette politique	4406
Détails de la politique	4406
Version de la politique	4407
Document de politique JSON	4407
En savoir plus	4408

CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy	4408
Utilisation de cette politique	4408
Détails de la politique	4408
Version de la politique	4409
Document de politique JSON	4409
En savoir plus	4411
CloudWatchNetworkMonitorServiceRolePolicy	4412
Utilisation de cette politique	4412
Détails de la politique	4412
Version de la politique	4412
Document de politique JSON	4412
En savoir plus	4414
CloudWatchOmniAWSIntegrationPolicy	4414
Utilisation de cette politique	4414
Détails de la politique	4414
Version de la politique	4414
Document de politique JSON	4414
En savoir plus	4427
CloudWatchOmniDomainAccessPolicy	4427
Utilisation de cette politique	4427
Détails de la politique	4427
Version de la politique	4427
Document de politique JSON	4428
En savoir plus	4428
CloudWatchOmniModelInferencePolicy	4429
Utilisation de cette politique	4429
Détails de la politique	4429
Version de la politique	4429
Document de politique JSON	4429
En savoir plus	4430
CloudWatchOmniSpaceAccessPolicy	4431
Utilisation de cette politique	4431
Détails de la politique	4431
Version de la politique	4431
Document de politique JSON	4431
En savoir plus	4442

CloudWatchOpenSearchDashboardAccess	4443
Utilisation de cette politique	4443
Détails de la politique	4443
Version de la politique	4443
Document de politique JSON	4443
En savoir plus	4446
CloudWatchOpenSearchDashboardsFullAccess	4446
Utilisation de cette politique	4446
Détails de la politique	4446
Version de la politique	4446
Document de politique JSON	4447
En savoir plus	4454
CloudWatchReadOnlyAccess	4454
Utilisation de cette politique	4454
Détails de la politique	4454
Version de la politique	4454
Document de politique JSON	4454
En savoir plus	4457
CloudWatchSyntheticsFullAccess	4458
Utilisation de cette politique	4458
Détails de la politique	4458
Version de la politique	4458
Document de politique JSON	4458
En savoir plus	4464
CloudWatchSyntheticsReadOnlyAccess	4464
Utilisation de cette politique	4464
Détails de la politique	4464
Version de la politique	4464
Document de politique JSON	4464
En savoir plus	4465
ComprehendDataAccessRolePolicy	4465
Utilisation de cette politique	4465
Détails de la politique	4465
Version de la politique	4466
Document de politique JSON	4466
En savoir plus	4466

ComprehendFullAccess	4466
Utilisation de cette politique	4467
Détails de la politique	4467
Version de la politique	4467
Document de politique JSON	4467
En savoir plus	4468
ComprehendMedicalFullAccess	4468
Utilisation de cette politique	4468
Détails de la politique	4468
Version de la politique	4468
Document de politique JSON	4468
En savoir plus	4469
ComprehendReadOnly	4469
Utilisation de cette politique	4469
Détails de la politique	4469
Version de la politique	4469
Document de politique JSON	4470
En savoir plus	4471
ComputeOptimizerAutomationServiceRolePolicy	4471
Utilisation de cette politique	4471
Détails de la politique	4471
Version de la politique	4472
Document de politique JSON	4472
En savoir plus	4474
ComputeOptimizerReadOnlyAccess	4474
Utilisation de cette politique	4474
Détails de la politique	4474
Version de la politique	4474
Document de politique JSON	4474
En savoir plus	4475
ComputeOptimizerServiceRolePolicy	4476
Utilisation de cette politique	4476
Détails de la politique	4476
Version de la politique	4476
Document de politique JSON	4476
En savoir plus	4479

ConfigConformsServiceRolePolicy	4479
Utilisation de cette politique	4479
Détails de la politique	4479
Version de la politique	4480
Document de politique JSON	4480
En savoir plus	4483
ConsoleFullAccessFromVercel	4483
Utilisation de cette politique	4483
Détails de la politique	4483
Version de la politique	4483
Document de politique JSON	4483
En savoir plus	4488
ConsoleViewOnlyAccessFromVercel	4488
Utilisation de cette politique	4488
Détails de la politique	4489
Version de la politique	4489
Document de politique JSON	4489
En savoir plus	4492
CostOptimizationHubAdminAccess	4492
Utilisation de cette politique	4492
Détails de la politique	4492
Version de la politique	4492
Document de politique JSON	4492
En savoir plus	4494
CostOptimizationHubReadOnlyAccess	4494
Utilisation de cette politique	4494
Détails de la politique	4494
Version de la politique	4494
Document de politique JSON	4495
En savoir plus	4495
CostOptimizationHubServiceRolePolicy	4495
Utilisation de cette politique	4495
Détails de la politique	4496
Version de la politique	4496
Document de politique JSON	4496
En savoir plus	4497

CustomerProfilesServiceLinkedRolePolicy	4497
Utilisation de cette politique	4497
Détails de la politique	4498
Version de la politique	4498
Document de politique JSON	4498
En savoir plus	4499
DatabaseAdministrator	4499
Utilisation de cette politique	4499
Détails de la politique	4500
Version de la politique	4500
Document de politique JSON	4500
En savoir plus	4503
DataScientist	4503
Utilisation de cette politique	4503
Détails de la politique	4503
Version de la politique	4503
Document de politique JSON	4503
En savoir plus	4508
DAXServiceRolePolicy	4508
Utilisation de cette politique	4508
Détails de la politique	4508
Version de la politique	4508
Document de politique JSON	4509
En savoir plus	4509
DBModDiscoveryAndAssessment	4509
Utilisation de cette politique	4510
Détails de la politique	4510
Version de la politique	4510
Document de politique JSON	4510
En savoir plus	4514
DBModProvisioningAndMigration	4514
Utilisation de cette politique	4514
Détails de la politique	4514
Version de la politique	4515
Document de politique JSON	4515
En savoir plus	4520

DBModVirtualSource	4520
Utilisation de cette politique	4520
Détails de la politique	4520
Version de la politique	4520
Document de politique JSON	4521
En savoir plus	4525
DeclarativePoliciesEC2Report	4525
Utilisation de cette politique	4525
Détails de la politique	4525
Version de la politique	4526
Document de politique JSON	4526
En savoir plus	4526
DynamoDBCloudWatchContributorInsightsServiceRolePolicy	4527
Utilisation de cette politique	4527
Détails de la politique	4527
Version de la politique	4527
Document de politique JSON	4527
En savoir plus	4528
DynamoDBGlobalTableSettingsManagementServiceRolePolicy	4528
Utilisation de cette politique	4528
Détails de la politique	4528
Version de la politique	4529
Document de politique JSON	4529
En savoir plus	4530
DynamoDBKinesisReplicationServiceRolePolicy	4530
Utilisation de cette politique	4530
Détails de la politique	4530
Version de la politique	4530
Document de politique JSON	4531
En savoir plus	4531
DynamoDBReplicationServiceRolePolicy	4531
Utilisation de cette politique	4532
Détails de la politique	4532
Version de la politique	4532
Document de politique JSON	4532
En savoir plus	4533

EC2ApplicationStatusChecksServiceRolePolicy	4533
Utilisation de cette politique	4534
Détails de la politique	4534
Version de la politique	4534
Document de politique JSON	4534
En savoir plus	4535
EC2FastLaunchFullAccess	4535
Utilisation de cette politique	4535
Détails de la politique	4536
Version de la politique	4536
Document de politique JSON	4536
En savoir plus	4543
EC2FastLaunchServiceRolePolicy	4544
Utilisation de cette politique	4544
Détails de la politique	4544
Version de la politique	4544
Document de politique JSON	4544
En savoir plus	4550
EC2FleetTimeShiftableServiceRolePolicy	4550
Utilisation de cette politique	4551
Détails de la politique	4551
Version de la politique	4551
Document de politique JSON	4551
En savoir plus	4553
Ec2ImageBuilderCrossAccountDistributionAccess	4553
Utilisation de cette politique	4553
Détails de la politique	4553
Version de la politique	4553
Document de politique JSON	4553
En savoir plus	4554
EC2ImageBuilderExecutionPolicy	4554
Utilisation de cette politique	4554
Détails de la politique	4554
Version de la politique	4555
Document de politique JSON	4555
En savoir plus	4570

EC2ImageBuilderLifecycleExecutionPolicy	4570
Utilisation de cette politique	4571
Détails de la politique	4571
Version de la politique	4571
Document de politique JSON	4571
En savoir plus	4573
EC2InstanceConnect	4573
Utilisation de cette politique	4573
Détails de la politique	4574
Version de la politique	4574
Document de politique JSON	4574
En savoir plus	4574
Ec2InstanceConnectEndpoint	4575
Utilisation de cette politique	4575
Détails de la politique	4575
Version de la politique	4575
Document de politique JSON	4575
En savoir plus	4578
EC2InstanceProfileForImageBuilder	4578
Utilisation de cette politique	4578
Détails de la politique	4578
Version de la politique	4578
Document de politique JSON	4579
En savoir plus	4581
EC2InstanceProfileForImageBuilderECRContainerBuilds	4582
Utilisation de cette politique	4582
Détails de la politique	4582
Version de la politique	4582
Document de politique JSON	4582
En savoir plus	4584
ECRReplicationServiceRolePolicy	4584
Utilisation de cette politique	4584
Détails de la politique	4584
Version de la politique	4584
Document de politique JSON	4585
En savoir plus	4585

ECRTemplateServiceRolePolicy	4585
Utilisation de cette politique	4585
Détails de la politique	4585
Version de la politique	4586
Document de politique JSON	4586
En savoir plus	4586
ElastiCacheServiceRolePolicy	4586
Utilisation de cette politique	4587
Détails de la politique	4587
Version de la politique	4587
Document de politique JSON	4587
En savoir plus	4589
ElasticLoadBalancingFullAccess	4589
Utilisation de cette politique	4589
Détails de la politique	4589
Version de la politique	4590
Document de politique JSON	4590
En savoir plus	4591
ElasticLoadBalancingReadOnly	4591
Utilisation de cette politique	4592
Détails de la politique	4592
Version de la politique	4592
Document de politique JSON	4592
En savoir plus	4593
ElementalActivationsDownloadSoftwareAccess	4593
Utilisation de cette politique	4594
Détails de la politique	4594
Version de la politique	4594
Document de politique JSON	4594
En savoir plus	4594
ElementalActivationsFullAccess	4595
Utilisation de cette politique	4595
Détails de la politique	4595
Version de la politique	4595
Document de politique JSON	4595
En savoir plus	4596

ElementalActivationsGenerateLicenses	4596
Utilisation de cette politique	4596
Détails de la politique	4596
Version de la politique	4596
Document de politique JSON	4597
En savoir plus	4597
ElementalActivationsReadOnlyAccess	4597
Utilisation de cette politique	4598
Détails de la politique	4598
Version de la politique	4598
Document de politique JSON	4598
En savoir plus	4598
ElementalAppliancesSoftwareFullAccess	4599
Utilisation de cette politique	4599
Détails de la politique	4599
Version de la politique	4599
Document de politique JSON	4599
En savoir plus	4600
ElementalAppliancesSoftwareReadOnlyAccess	4600
Utilisation de cette politique	4600
Détails de la politique	4600
Version de la politique	4600
Document de politique JSON	4601
En savoir plus	4601
ElementalSupportCenterFullAccess	4601
Utilisation de cette politique	4601
Détails de la politique	4602
Version de la politique	4602
Document de politique JSON	4602
En savoir plus	4602
EMRDescribeClusterPolicyForEMRWAL	4603
Utilisation de cette politique	4603
Détails de la politique	4603
Version de la politique	4603
Document de politique JSON	4603
En savoir plus	4604

EndUserMessagingServiceRolePolicy	4604
Utilisation de cette politique	4604
Détails de la politique	4604
Version de la politique	4604
Document de politique JSON	4605
En savoir plus	4605
FinOpsAgentAgentPolicy	4605
Utilisation de cette politique	4605
Détails de la politique	4605
Version de la politique	4606
Document de politique JSON	4606
En savoir plus	4610
FinOpsAgentOperatorPolicy	4610
Utilisation de cette politique	4610
Détails de la politique	4610
Version de la politique	4611
Document de politique JSON	4611
En savoir plus	4612
FMSServiceRolePolicy	4612
Utilisation de cette politique	4612
Détails de la politique	4612
Version de la politique	4613
Document de politique JSON	4613
En savoir plus	4629
FSxDeleteServiceLinkedRoleAccess	4630
Utilisation de cette politique	4630
Détails de la politique	4630
Version de la politique	4630
Document de politique JSON	4630
En savoir plus	4631
GameLiftContainerFleetPolicy	4631
Utilisation de cette politique	4631
Détails de la politique	4631
Version de la politique	4631
Document de politique JSON	4632
En savoir plus	4633

GameLiftGameServerGroupPolicy	4633
Utilisation de cette politique	4633
Détails de la politique	4633
Version de la politique	4633
Document de politique JSON	4634
En savoir plus	4635
GitLabDuoWithAmazonQPermissionsPolicy	4635
Utilisation de cette politique	4636
Détails de la politique	4636
Version de la politique	4636
Document de politique JSON	4636
En savoir plus	4637
GlobalAcceleratorFullAccess	4637
Utilisation de cette politique	4637
Détails de la politique	4638
Version de la politique	4638
Document de politique JSON	4638
En savoir plus	4639
GlobalAcceleratorReadOnlyAccess	4639
Utilisation de cette politique	4639
Détails de la politique	4639
Version de la politique	4640
Document de politique JSON	4640
En savoir plus	4640
GreengrassOTAUpdateArtifactAccess	4640
Utilisation de cette politique	4641
Détails de la politique	4641
Version de la politique	4641
Document de politique JSON	4641
En savoir plus	4642
GroundTruthSyntheticConsoleFullAccess	4642
Utilisation de cette politique	4642
Détails de la politique	4642
Version de la politique	4642
Document de politique JSON	4643
En savoir plus	4643

GroundTruthSyntheticConsoleReadOnlyAccess	4643
Utilisation de cette politique	4643
Détails de la politique	4643
Version de la politique	4644
Document de politique JSON	4644
En savoir plus	4644
Health_OrganizationsServiceRolePolicy	4644
Utilisation de cette politique	4645
Détails de la politique	4645
Version de la politique	4645
Document de politique JSON	4645
En savoir plus	4646
IAMAccessAdvisorReadOnly	4646
Utilisation de cette politique	4646
Détails de la politique	4646
Version de la politique	4646
Document de politique JSON	4646
En savoir plus	4647
IAMAccessAnalyzerFullAccess	4648
Utilisation de cette politique	4648
Détails de la politique	4648
Version de la politique	4648
Document de politique JSON	4648
En savoir plus	4649
IAMAccessAnalyzerReadOnlyAccess	4649
Utilisation de cette politique	4650
Détails de la politique	4650
Version de la politique	4650
Document de politique JSON	4650
En savoir plus	4651
IAMFullAccess	4651
Utilisation de cette politique	4651
Détails de la politique	4651
Version de la politique	4651
Document de politique JSON	4651
En savoir plus	4652

IAMReadOnlyAccess	4652
Utilisation de cette politique	4652
Détails de la politique	4652
Version de la politique	4653
Document de politique JSON	4653
En savoir plus	4653
IAMSelfManageServiceSpecificCredentials	4654
Utilisation de cette politique	4654
Détails de la politique	4654
Version de la politique	4654
Document de politique JSON	4654
En savoir plus	4655
IAMUserChangePassword	4655
Utilisation de cette politique	4655
Détails de la politique	4655
Version de la politique	4655
Document de politique JSON	4656
En savoir plus	4656
IAMUserSSHKeys	4656
Utilisation de cette politique	4657
Détails de la politique	4657
Version de la politique	4657
Document de politique JSON	4657
En savoir plus	4658
IVSFullAccess	4658
Utilisation de cette politique	4658
Détails de la politique	4658
Version de la politique	4658
Document de politique JSON	4658
En savoir plus	4659
IVSReadOnlyAccess	4659
Utilisation de cette politique	4659
Détails de la politique	4659
Version de la politique	4660
Document de politique JSON	4660
En savoir plus	4661

IVSRecordToS3	4661
Utilisation de cette politique	4661
Détails de la politique	4661
Version de la politique	4662
Document de politique JSON	4662
En savoir plus	4662
KafkaConnectServiceRolePolicy	4662
Utilisation de cette politique	4662
Détails de la politique	4663
Version de la politique	4663
Document de politique JSON	4663
En savoir plus	4664
KafkaServiceRolePolicy	4665
Utilisation de cette politique	4665
Détails de la politique	4665
Version de la politique	4665
Document de politique JSON	4665
En savoir plus	4667
KeyspacesCDCServiceRolePolicy	4667
Utilisation de cette politique	4667
Détails de la politique	4667
Version de la politique	4668
Document de politique JSON	4668
En savoir plus	4668
KeyspacesReplicationServiceRolePolicy	4669
Utilisation de cette politique	4669
Détails de la politique	4669
Version de la politique	4669
Document de politique JSON	4669
En savoir plus	4671
LakeFormationDataAccessServiceRolePolicy	4671
Utilisation de cette politique	4671
Détails de la politique	4671
Version de la politique	4671
Document de politique JSON	4671
En savoir plus	4672

LexBotPolicy	4672
Utilisation de cette politique	4672
Détails de la politique	4672
Version de la politique	4673
Document de politique JSON	4673
En savoir plus	4673
LexChannelPolicy	4674
Utilisation de cette politique	4674
Détails de la politique	4674
Version de la politique	4674
Document de politique JSON	4674
En savoir plus	4675
LightsailExportAccess	4675
Utilisation de cette politique	4675
Détails de la politique	4675
Version de la politique	4675
Document de politique JSON	4675
En savoir plus	4676
MediaConnectGatewayInstanceRolePolicy	4676
Utilisation de cette politique	4677
Détails de la politique	4677
Version de la politique	4677
Document de politique JSON	4677
En savoir plus	4678
MediaPackageServiceRolePolicy	4678
Utilisation de cette politique	4678
Détails de la politique	4678
Version de la politique	4678
Document de politique JSON	4678
En savoir plus	4679
MemoryDBServiceRolePolicy	4679
Utilisation de cette politique	4679
Détails de la politique	4679
Version de la politique	4680
Document de politique JSON	4680
En savoir plus	4682

MigrationHubDMSAccessServiceRolePolicy	4682
Utilisation de cette politique	4682
Détails de la politique	4682
Version de la politique	4683
Document de politique JSON	4683
En savoir plus	4684
MigrationHubServiceRolePolicy	4684
Utilisation de cette politique	4684
Détails de la politique	4684
Version de la politique	4684
Document de politique JSON	4685
En savoir plus	4686
MigrationHubSMSAccessServiceRolePolicy	4686
Utilisation de cette politique	4686
Détails de la politique	4686
Version de la politique	4687
Document de politique JSON	4687
En savoir plus	4688
MonitronServiceRolePolicy	4688
Utilisation de cette politique	4688
Détails de la politique	4688
Version de la politique	4688
Document de politique JSON	4689
En savoir plus	4689
MultiPartyApprovalFullAccess	4689
Utilisation de cette politique	4689
Détails de la politique	4689
Version de la politique	4690
Document de politique JSON	4690
En savoir plus	4692
MultiPartyApprovalReadOnlyAccess	4692
Utilisation de cette politique	4693
Détails de la politique	4693
Version de la politique	4693
Document de politique JSON	4693
En savoir plus	4695

NeptuneConsoleFullAccess	4695
Utilisation de cette politique	4695
Détails de la politique	4695
Version de la politique	4696
Document de politique JSON	4696
En savoir plus	4701
NeptuneFullAccess	4701
Utilisation de cette politique	4702
Détails de la politique	4702
Version de la politique	4702
Document de politique JSON	4702
En savoir plus	4706
NeptuneGraphReadOnlyAccess	4706
Utilisation de cette politique	4706
Détails de la politique	4707
Version de la politique	4707
Document de politique JSON	4707
En savoir plus	4708
NeptuneReadOnlyAccess	4709
Utilisation de cette politique	4709
Détails de la politique	4709
Version de la politique	4709
Document de politique JSON	4709
En savoir plus	4711
NetworkAdministrator	4712
Utilisation de cette politique	4712
Détails de la politique	4712
Version de la politique	4712
Document de politique JSON	4712
En savoir plus	4720
NetworkSecurityDirectorServiceLinkedRolePolicy	4720
Utilisation de cette politique	4720
Détails de la politique	4720
Version de la politique	4720
Document de politique JSON	4721
En savoir plus	4726

NetworkSecurityManagerServiceRolePolicy	4726
Utilisation de cette politique	4726
Détails de la politique	4726
Version de la politique	4727
Document de politique JSON	4727
En savoir plus	4735
NovaActServiceRolePolicy	4736
Utilisation de cette politique	4736
Détails de la politique	4736
Version de la politique	4736
Document de politique JSON	4736
En savoir plus	4737
OAMFullAccess	4737
Utilisation de cette politique	4737
Détails de la politique	4737
Version de la politique	4737
Document de politique JSON	4738
En savoir plus	4738
OAMReadOnlyAccess	4738
Utilisation de cette politique	4738
Détails de la politique	4738
Version de la politique	4739
Document de politique JSON	4739
En savoir plus	4739
OpensearchIngestionSelfManagedVpcePolicy	4739
Utilisation de cette politique	4740
Détails de la politique	4740
Version de la politique	4740
Document de politique JSON	4740
En savoir plus	4741
PartnerCentralAccountManagementUserRoleAssociation	4741
Utilisation de cette politique	4741
Détails de la politique	4741
Version de la politique	4741
Document de politique JSON	4742
En savoir plus	4742

PartnerCentralIncentiveBenefitManagement	4743
Utilisation de cette politique	4743
Détails de la politique	4743
Version de la politique	4743
Document de politique JSON	4743
En savoir plus	4747
PowerUserAccess	4747
Utilisation de cette politique	4747
Détails de la politique	4747
Version de la politique	4748
Document de politique JSON	4748
En savoir plus	4749
PricingPlanManagerFullAccess	4749
Utilisation de cette politique	4749
Détails de la politique	4749
Version de la politique	4749
Document de politique JSON	4749
En savoir plus	4750
PricingPlanManagerReadOnlyAccess	4750
Utilisation de cette politique	4750
Détails de la politique	4751
Version de la politique	4751
Document de politique JSON	4751
En savoir plus	4751
QAppsServiceRolePolicy	4752
Utilisation de cette politique	4752
Détails de la politique	4752
Version de la politique	4752
Document de politique JSON	4752
En savoir plus	4753
QBusinessQuicksightPluginPolicy	4753
Utilisation de cette politique	4753
Détails de la politique	4753
Version de la politique	4753
Document de politique JSON	4754
En savoir plus	4754

QBusinessServiceRolePolicy	4754
Utilisation de cette politique	4754
Détails de la politique	4755
Version de la politique	4755
Document de politique JSON	4755
En savoir plus	4757
QuickSightAccessForS3StorageManagementAnalyticsReadOnly	4757
Utilisation de cette politique	4757
Détails de la politique	4757
Version de la politique	4757
Document de politique JSON	4757
En savoir plus	4758
RDSCloudHsmAuthorizationRole	4758
Utilisation de cette politique	4758
Détails de la politique	4759
Version de la politique	4759
Document de politique JSON	4759
En savoir plus	4759
ReadOnlyAccess	4760
Utilisation de cette politique	4760
Détails de la politique	4760
Version de la politique	4760
Document de politique JSON	4760
En savoir plus	4830
ReInventTicketApprovalAccess	4830
Utilisation de cette politique	4830
Détails de la politique	4830
Version de la politique	4830
Document de politique JSON	4831
En savoir plus	4831
ResourceGroupsandTagEditorFullAccess	4831
Utilisation de cette politique	4831
Détails de la politique	4831
Version de la politique	4832
Document de politique JSON	4832
En savoir plus	4832

ResourceGroupsandTagEditorReadOnlyAccess	4833
Utilisation de cette politique	4833
Détails de la politique	4833
Version de la politique	4833
Document de politique JSON	4833
En savoir plus	4834
ResourceGroupsServiceRolePolicy	4834
Utilisation de cette politique	4834
Détails de la politique	4834
Version de la politique	4835
Document de politique JSON	4835
En savoir plus	4835
ResourceGroupsTaggingAPITagUntagSupportedResources	4835
Utilisation de cette politique	4836
Détails de la politique	4836
Version de la politique	4836
Document de politique JSON	4836
En savoir plus	4844
ROSAAmazonEBSCSIDriverOperatorPolicy	4845
Utilisation de cette politique	4845
Détails de la politique	4845
Version de la politique	4845
Document de politique JSON	4845
En savoir plus	4853
ROSACloudNetworkConfigOperatorPolicy	4854
Utilisation de cette politique	4854
Détails de la politique	4854
Version de la politique	4854
Document de politique JSON	4854
En savoir plus	4855
ROSAControlPlaneOperatorPolicy	4855
Utilisation de cette politique	4856
Détails de la politique	4856
Version de la politique	4856
Document de politique JSON	4856
En savoir plus	4861

ROSAImageRegistryOperatorPolicy	4861
Utilisation de cette politique	4862
Détails de la politique	4862
Version de la politique	4862
Document de politique JSON	4862
En savoir plus	4863
ROSAIngressOperatorPolicy	4864
Utilisation de cette politique	4864
Détails de la politique	4864
Version de la politique	4864
Document de politique JSON	4864
En savoir plus	4865
ROSAInstallerPolicy	4865
Utilisation de cette politique	4865
Détails de la politique	4866
Version de la politique	4866
Document de politique JSON	4866
En savoir plus	4874
ROSAKarpenterControllerPolicy	4875
Utilisation de cette politique	4875
Détails de la politique	4875
Version de la politique	4875
Document de politique JSON	4875
En savoir plus	4882
ROSAKMSPProviderPolicy	4882
Utilisation de cette politique	4882
Détails de la politique	4882
Version de la politique	4882
Document de politique JSON	4883
En savoir plus	4883
ROSAKubeControllerPolicy	4883
Utilisation de cette politique	4883
Détails de la politique	4884
Version de la politique	4884
Document de politique JSON	4884
En savoir plus	4889

ROSAManageSubscription	4889
Utilisation de cette politique	4889
Détails de la politique	4889
Version de la politique	4889
Document de politique JSON	4890
En savoir plus	4890
ROSANodePoolManagementPolicy	4891
Utilisation de cette politique	4891
Détails de la politique	4891
Version de la politique	4891
Document de politique JSON	4891
En savoir plus	4898
ROSASharedVPCEndpointPolicy	4898
Utilisation de cette politique	4898
Détails de la politique	4898
Version de la politique	4898
Document de politique JSON	4899
En savoir plus	4902
ROSASharedVPCRoute53Policy	4903
Utilisation de cette politique	4903
Détails de la politique	4903
Version de la politique	4903
Document de politique JSON	4903
En savoir plus	4904
ROSASRESupportPolicy	4905
Utilisation de cette politique	4905
Détails de la politique	4905
Version de la politique	4905
Document de politique JSON	4905
En savoir plus	4910
ROSAWorkerInstancePolicy	4910
Utilisation de cette politique	4910
Détails de la politique	4911
Version de la politique	4911
Document de politique JSON	4911
En savoir plus	4912

Route53RecoveryReadinessServiceRolePolicy	4912
Utilisation de cette politique	4912
Détails de la politique	4913
Version de la politique	4913
Document de politique JSON	4913
En savoir plus	4916
Route53ResolverServiceRolePolicy	4917
Utilisation de cette politique	4917
Détails de la politique	4917
Version de la politique	4917
Document de politique JSON	4917
En savoir plus	4918
RTBFabricServiceRolePolicy	4918
Utilisation de cette politique	4918
Détails de la politique	4918
Version de la politique	4918
Document de politique JSON	4919
En savoir plus	4921
S3StorageLensServiceRolePolicy	4921
Utilisation de cette politique	4921
Détails de la politique	4921
Version de la politique	4921
Document de politique JSON	4922
En savoir plus	4922
SageMakerStudioAdminIAMConsolePolicy	4922
Utilisation de cette politique	4923
Détails de la politique	4923
Version de la politique	4923
Document de politique JSON	4923
En savoir plus	4935
SageMakerStudioAdminIAMDefaultExecutionPolicy	4935
Utilisation de cette politique	4936
Détails de la politique	4936
Version de la politique	4936
Document de politique JSON	4936
En savoir plus	4961

SageMakerStudioAdminIAMPermissiveExecutionPolicy	4962
Utilisation de cette politique	4962
Détails de la politique	4962
Version de la politique	4962
Document de politique JSON	4962
En savoir plus	4981
SageMakerStudioAdminProjectUserRolePolicy	4981
Utilisation de cette politique	4981
Détails de la politique	4982
Version de la politique	4982
Document de politique JSON	4982
En savoir plus	4984
SageMakerStudioBedrockAgentServiceRolePolicy	4985
Utilisation de cette politique	4985
Détails de la politique	4985
Version de la politique	4985
Document de politique JSON	4985
En savoir plus	4989
SageMakerStudioBedrockChatAgentUserRolePolicy	4989
Utilisation de cette politique	4989
Détails de la politique	4989
Version de la politique	4989
Document de politique JSON	4990
En savoir plus	4994
SageMakerStudioBedrockEvaluationJobServiceRolePolicy	4994
Utilisation de cette politique	4994
Détails de la politique	4994
Version de la politique	4994
Document de politique JSON	4995
En savoir plus	4998
SageMakerStudioBedrockFlowServiceRolePolicy	4998
Utilisation de cette politique	4999
Détails de la politique	4999
Version de la politique	4999
Document de politique JSON	4999
En savoir plus	5003

SageMakerStudioBedrockFunctionExecutionRolePolicy	5003
Utilisation de cette politique	5003
Détails de la politique	5003
Version de la politique	5004
Document de politique JSON	5004
En savoir plus	5005
SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy	5005
Utilisation de cette politique	5005
Détails de la politique	5005
Version de la politique	5006
Document de politique JSON	5006
En savoir plus	5007
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy	5007
Utilisation de cette politique	5007
Détails de la politique	5007
Version de la politique	5007
Document de politique JSON	5008
En savoir plus	5013
SageMakerStudioBedrockPromptUserRolePolicy	5013
Utilisation de cette politique	5014
Détails de la politique	5014
Version de la politique	5014
Document de politique JSON	5014
En savoir plus	5016
SageMakerStudioDomainExecutionRolePolicy	5017
Utilisation de cette politique	5017
Détails de la politique	5017
Version de la politique	5017
Document de politique JSON	5017
En savoir plus	5024
SageMakerStudioDomainServiceRolePolicy	5024
Utilisation de cette politique	5024
Détails de la politique	5024
Version de la politique	5024
Document de politique JSON	5025
En savoir plus	5026

SageMakerStudioEMRContainersSystemNamespaceRolePolicy	5026
Utilisation de cette politique	5026
Détails de la politique	5026
Version de la politique	5026
Document de politique JSON	5027
En savoir plus	5028
SageMakerStudioEMRInstanceRolePolicy	5028
Utilisation de cette politique	5029
Détails de la politique	5029
Version de la politique	5029
Document de politique JSON	5029
En savoir plus	5033
SageMakerStudioEMRServiceRolePolicy	5033
Utilisation de cette politique	5033
Détails de la politique	5033
Version de la politique	5033
Document de politique JSON	5034
En savoir plus	5036
SageMakerStudioFullAccess	5036
Utilisation de cette politique	5036
Détails de la politique	5036
Version de la politique	5036
Document de politique JSON	5037
En savoir plus	5047
SageMakerStudioProjectProvisioningRolePolicy	5047
Utilisation de cette politique	5047
Détails de la politique	5047
Version de la politique	5047
Document de politique JSON	5048
En savoir plus	5117
SageMakerStudioProjectRoleMachineLearningPolicy	5117
Utilisation de cette politique	5117
Détails de la politique	5117
Version de la politique	5118
Document de politique JSON	5118
En savoir plus	5148

SageMakerStudioProjectUserRolePermissionsBoundary	5148
Utilisation de cette politique	5149
Détails de la politique	5149
Version de la politique	5149
Document de politique JSON	5149
En savoir plus	5204
SageMakerStudioProjectUserRolePolicy	5205
Utilisation de cette politique	5205
Détails de la politique	5205
Version de la politique	5205
Document de politique JSON	5205
En savoir plus	5271
SageMakerStudioQueryExecutionRolePolicy	5271
Utilisation de cette politique	5272
Détails de la politique	5272
Version de la politique	5272
Document de politique JSON	5272
En savoir plus	5274
SageMakerStudioUserIAMConsolePolicy	5274
Utilisation de cette politique	5274
Détails de la politique	5274
Version de la politique	5275
Document de politique JSON	5275
En savoir plus	5276
SageMakerStudioUserIAMDefaultExecutionPolicy	5277
Utilisation de cette politique	5277
Détails de la politique	5277
Version de la politique	5277
Document de politique JSON	5277
En savoir plus	5302
SageMakerStudioUserIAMPermissiveExecutionPolicy	5302
Utilisation de cette politique	5302
Détails de la politique	5302
Version de la politique	5303
Document de politique JSON	5303
En savoir plus	5317

SecretsManagerReadWrite	5318
Utilisation de cette politique	5318
Détails de la politique	5318
Version de la politique	5318
Document de politique JSON	5318
En savoir plus	5320
SecurityAgentWebAppAPIPolicy	5320
Utilisation de cette politique	5321
Détails de la politique	5321
Version de la politique	5321
Document de politique JSON	5321
En savoir plus	5323
SecurityAgentWebAppPolicy	5323
Utilisation de cette politique	5323
Détails de la politique	5323
Version de la politique	5323
Document de politique JSON	5324
En savoir plus	5325
SecurityAudit	5325
Utilisation de cette politique	5326
Détails de la politique	5326
Version de la politique	5326
Document de politique JSON	5326
En savoir plus	5355
SecurityLakeResourceManagementServiceRolePolicy	5355
Utilisation de cette politique	5355
Détails de la politique	5355
Version de la politique	5355
Document de politique JSON	5356
En savoir plus	5361
SecurityLakeServiceLinkedRole	5361
Utilisation de cette politique	5361
Détails de la politique	5362
Version de la politique	5362
Document de politique JSON	5362
En savoir plus	5365

ServerMigration_ServiceRole	5365
Utilisation de cette politique	5365
Détails de la politique	5365
Version de la politique	5366
Document de politique JSON	5366
En savoir plus	5371
ServerMigrationConnector	5371
Utilisation de cette politique	5371
Détails de la politique	5371
Version de la politique	5371
Document de politique JSON	5372
En savoir plus	5373
ServerMigrationServiceConsoleFullAccess	5373
Utilisation de cette politique	5374
Détails de la politique	5374
Version de la politique	5374
Document de politique JSON	5374
En savoir plus	5376
ServerMigrationServiceLaunchRole	5376
Utilisation de cette politique	5376
Détails de la politique	5376
Version de la politique	5376
Document de politique JSON	5377
En savoir plus	5379
ServerMigrationServiceRoleForInstanceValidation	5380
Utilisation de cette politique	5380
Détails de la politique	5380
Version de la politique	5380
Document de politique JSON	5380
En savoir plus	5381
ServiceQuotasFullAccess	5381
Utilisation de cette politique	5381
Détails de la politique	5381
Version de la politique	5381
Document de politique JSON	5382
En savoir plus	5383

ServiceQuotasReadOnlyAccess	5384
Utilisation de cette politique	5384
Détails de la politique	5384
Version de la politique	5384
Document de politique JSON	5384
En savoir plus	5386
ServiceQuotasServiceRolePolicy	5386
Utilisation de cette politique	5386
Détails de la politique	5386
Version de la politique	5386
Document de politique JSON	5386
En savoir plus	5387
SignInLocalDevelopmentAccess	5387
Utilisation de cette politique	5387
Détails de la politique	5387
Version de la politique	5387
Document de politique JSON	5388
En savoir plus	5388
SimpleWorkflowFullAccess	5388
Utilisation de cette politique	5388
Détails de la politique	5389
Version de la politique	5389
Document de politique JSON	5389
En savoir plus	5389
SMSVoiceServiceRolePolicy	5390
Utilisation de cette politique	5390
Détails de la politique	5390
Version de la politique	5390
Document de politique JSON	5390
En savoir plus	5391
SplitCostAllocationDataServiceRolePolicy	5391
Utilisation de cette politique	5391
Détails de la politique	5391
Version de la politique	5391
Document de politique JSON	5392
En savoir plus	5392

SSMQuickSetupRolePolicy	5392
Utilisation de cette politique	5393
Détails de la politique	5393
Version de la politique	5393
Document de politique JSON	5393
En savoir plus	5396
SupportUser	5396
Utilisation de cette politique	5396
Détails de la politique	5396
Version de la politique	5397
Document de politique JSON	5397
En savoir plus	5402
SystemAdministrator	5402
Utilisation de cette politique	5402
Détails de la politique	5402
Version de la politique	5403
Document de politique JSON	5403
En savoir plus	5409
TranslateFullAccess	5409
Utilisation de cette politique	5409
Détails de la politique	5409
Version de la politique	5410
Document de politique JSON	5410
En savoir plus	5410
TranslateReadOnly	5411
Utilisation de cette politique	5411
Détails de la politique	5411
Version de la politique	5411
Document de politique JSON	5411
En savoir plus	5412
ViewOnlyAccess	5412
Utilisation de cette politique	5412
Détails de la politique	5412
Version de la politique	5412
Document de politique JSON	5413
En savoir plus	5430

VMImportExportRoleForAWSConnector	5430
Utilisation de cette politique	5430
Détails de la politique	5431
Version de la politique	5431
Document de politique JSON	5431
En savoir plus	5432
VPCLatticeFullAccess	5432
Utilisation de cette politique	5432
Détails de la politique	5432
Version de la politique	5432
Document de politique JSON	5433
En savoir plus	5435
VPCLatticeReadOnlyAccess	5435
Utilisation de cette politique	5435
Détails de la politique	5435
Version de la politique	5435
Document de politique JSON	5435
En savoir plus	5436
VPCLatticeServicesInvokeAccess	5437
Utilisation de cette politique	5437
Détails de la politique	5437
Version de la politique	5437
Document de politique JSON	5437
En savoir plus	5438
WAFLoggingServiceRolePolicy	5438
Utilisation de cette politique	5438
Détails de la politique	5438
Version de la politique	5438
Document de politique JSON	5438
En savoir plus	5439
WAFRegionalLoggingServiceRolePolicy	5439
Utilisation de cette politique	5440
Détails de la politique	5440
Version de la politique	5440
Document de politique JSON	5440
En savoir plus	5441

WAFV2LoggingServiceRolePolicy	5441
Utilisation de cette politique	5441
Détails de la politique	5441
Version de la politique	5442
Document de politique JSON	5442
En savoir plus	5443
WellArchitectedAgentResourceScanning	5443
Utilisation de cette politique	5443
Détails de la politique	5443
Version de la politique	5443
Document de politique JSON	5444
En savoir plus	5470
WellArchitectedConsoleFullAccess	5470
Utilisation de cette politique	5470
Détails de la politique	5470
Version de la politique	5470
Document de politique JSON	5470
En savoir plus	5473
WellArchitectedConsoleReadOnlyAccess	5473
Utilisation de cette politique	5473
Détails de la politique	5473
Version de la politique	5474
Document de politique JSON	5474
En savoir plus	5474
WorkLinkServiceRolePolicy	5475
Utilisation de cette politique	5475
Détails de la politique	5475
Version de la politique	5475
Document de politique JSON	5475
En savoir plus	5476
.....	5477

Que sont les politiques AWS gérées ?

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants. Ils vous permettent de commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles plus facilement que si vous deviez rédiger vous-même les politiques.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont disponibles pour tous AWS les clients. Nous vous recommandons de réduire encore les autorisations en définissant des [politiques gérées par le client](#) qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'un nouveau AWS service est lancé ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez [Politiques gérées par AWS](#) dans le Guide de l'utilisateur IAM.

Comprendre les pages de référence des politiques

Chaque page de référence des politiques inclut les informations suivantes :

- Utilisation de cette politique : si vous pouvez associer la politique aux utilisateurs, aux groupes et aux rôles
- Détails de la politique
 - Type : type de politique AWS gérée
 - `AWS managed policy`— Une politique AWS gérée standard
 - `Job function policy`— Politique alignée sur les fonctions professionnelles courantes de l'industrie
 - `Service-linked role policy`— Politique attachée à un rôle lié à un service qui permet à un service d'effectuer des actions en votre nom, telles que [the section called “AmazonRDSPreviewServiceRolePolicy”](#)

- **Service role policy**— Politique conçue pour fonctionner avec les rôles de service, tels que [the section called “AWSControlTowerServiceRolePolicy”](#)
- **Heure de création** : date à laquelle la politique a été créée pour la première fois
- **Heure de modification** : date à laquelle cette version de la politique a été modifiée
- **ARN** — Le nom de ressource Amazon de la politique
- **Version de la politique** : version des autorisations accordées par la politique
- **Document de politique JSON** — La politique JSON
- **En savoir plus** — Liens vers la documentation relative aux politiques AWS gérées

Politiques gérées déconseillées AWS

AWS met régulièrement à jour les politiques AWS gérées. Dans la plupart des cas, nous ajoutons des autorisations à une politique. Cela se produit lorsque nous lançons un nouveau service ou une nouvelle fonctionnalité. Pour améliorer la sécurité des politiques AWS gérées, nous réduisons parfois le champ d'application des politiques. Lorsque nous supprimons des autorisations d'une politique, nous la définissons comme obsolète et nous en rendons une nouvelle disponible. Lorsque vous AWS dépréciez un service ou une fonctionnalité, nous désapprouvons également la politique AWS gérée pour cette fonctionnalité.

Si vous recevez une notification par e-mail indiquant qu'une politique que vous utilisez est obsolète, nous vous recommandons d'agir immédiatement. Identifiez le changement apporté à la politique et mettez à jour vos flux de travail. S'il AWS fournit une politique de remplacement, prévoyez de l'associer à toutes les identités concernées (utilisateurs, groupes et rôles), puis de détacher la politique obsolète de ces identités.

Les caractéristiques d'une politique obsolète sont les suivantes :

- Il est supprimé de ce guide.
- Les autorisations continuent de fonctionner pour toutes les identités actuellement associées.
- Dans les comptes où la politique est associée à une identité, elle apparaît dans la liste des politiques de la console IAM avec une icône d'avertissement à côté.
- Il ne peut être rattaché à aucune nouvelle identité. Si vous le détachez d'une identité actuelle, vous ne pouvez pas le rattacher.
- Une fois que vous l'avez détaché de toutes les entités actuelles, il n'est plus visible.

AWS stratégies gérées

AWS politiques gérées

- [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](#)
- [Gestion des PC Amazon DRS](#)
- [AmazonDynamoDBFullAccess](#)

- [AmazonDynamoDBFullAccess_v2](#)
- [AmazonDynamoDBFullAccesswithDataPipeline](#)
- [AmazonDynamoDBReadOnlyAccess](#)
- [AmazonEBSCSIDriverEKSClusterScopedPolicy](#)
- [AmazonEBSCSIDriverPolicy](#)
- [AmazonEBSCSIDriverPolicyV2](#)
- [AmazonEC2ContainerRegistryFullAccess](#)
- [AmazonEC2ContainerRegistryPowerUser](#)
- [AmazonEC2ContainerRegistryPullOnly](#)
- [AmazonEC2ContainerRegistryReadOnly](#)
- [AmazonEC2ContainerServiceAutoscaleRole](#)
- [AmazonEC2ContainerServiceEventsRole](#)
- [AmazonEC2ContainerServiceforEC2Role](#)
- [AmazonEC2ContainerServiceRole](#)
- [AmazonEC2FullAccess](#)
- [AmazonEC2ImageReferencesAccessPolicy](#)
- [AmazonEC2ReadOnlyAccess](#)
- [AmazonEC2RoleforAWSCodeDeploy](#)
- [AmazonEC2RoleforAWSCodeDeployLimited](#)
- [AmazonEC2RoleforDataPipelineRole](#)
- [Rôle Amazon EC2 pour SSM](#)
- [AmazonEC2RolePolicyForLaunchWizard](#)
- [AmazonEC2SpotFleetAutoscaleRole](#)
- [AmazonEC2SpotFleetTaggingRole](#)
- [Amazon ECS_ FullAccess](#)
- [AmazonECSComputeServiceRolePolicy](#)
- [AmazonECSInfrastructureRoleforExpressGatewayServices](#)
- [AmazonECSInfrastructureRoleForGatewayHostSharedALB](#)
- [AmazonECSInfrastructureRolePolicyForLoadBalancers](#)

- [AmazonECSInfrastructureRolePolicyForManagedInstances](#)
- [AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity](#)
- [AmazonECSInfrastructureRolePolicyForVolumes](#)
- [AmazonECSInfrastructureRolePolicyForVpcLattice](#)
- [AmazonECSInstanceRolePolicyForManagedInstances](#)
- [AmazonECSServiceRolePolicy](#)
- [AmazonECSTaskExecutionRolePolicy](#)
- [AmazonEFSCSIDriverPolicy](#)
- [AmazonEKS_CNI_Policy](#)
- [AmazonEKSBlockStoragePolicy](#)
- [AmazonEKSBlockStoragePolicyV2](#)
- [AmazonEKSClusterPolicy](#)
- [AmazonEKSComputePolicy](#)
- [AmazonEKSConectorServiceRolePolicy](#)
- [AmazonEKSDashboardConsoleReadOnly](#)
- [AmazonEKSDashboardServiceRolePolicy](#)
- [AmazonEKSFargatePodExecutionRolePolicy](#)
- [AmazonEKSTaskExecutionRolePolicy](#)
- [AmazonEKSLoadBalancingPolicy](#)
- [AmazonEKSLocalOutpostClusterPolicy](#)
- [AmazonEKSLocalOutpostServiceRolePolicy](#)
- [AmazonEKSMCPRReadOnlyAccess](#)
- [AmazonEKSNetworkingPolicy](#)
- [AmazonEKSServicePolicy](#)
- [AmazonEKSServiceRolePolicy](#)
- [AmazonEKSVPCResourceController](#)
- [AmazonEKSWorkerNodeMinimalPolicy](#)
- [AmazonEKSWorkerNodePolicy](#)
- [AmazonElastiCacheFullAccess](#)

- [AmazonElasticCacheReadOnlyAccess](#)
- [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_Accès complet](#)
- [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](#)
- [AmazonRDSDDataFullAccess](#)
- [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](#)
- [AmazonSageMakerCanvasSMDDataScienceAssistantAccess](#)
- [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](#)
- [AmazonSESEFullAccess](#)
- [AmazonSESReadOnlyAccess](#)
- [AmazonSESServiceRolePolicy](#)
- [AmazonSNSFullAccess](#)
- [AmazonSNSReadOnlyAccess](#)
- [Rôle Amazon SNS](#)
- [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](#)
- [AWSBCMDDataExportsServiceRolePolicy](#)
- [AWSBedrockAgentCoreGatewayNetworkServiceRolePolicy](#)
- [AWSBedrockAgentCoreIdentityNetworkServiceRolePolicy](#)
- [AWSBedrockAgentCoreRuntimeInstancesServiceRolePolicy](#)

- [AWSBillingConductorFullAccess](#)
- [AWSBillingConductorReadOnlyAccess](#)
- [AWSBillingConductorRolePolicy](#)
- [AWSBillingReadOnlyAccess](#)
- [AWSBillingServiceRolePolicy](#)
- [AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM](#)
- [AWSBudgetsActionsWithAWSResourceControlAccess](#)
- [AWSBudgetsReadOnlyAccess](#)
- [AWSBudgetsSpendLimitMemberRolePolicy](#)
- [AWSBugBustFullAccess](#)
- [AWSBugBustPlayerAccess](#)
- [AWSBugBustServiceRolePolicy](#)
- [AWSCertificateManagerFullAccess](#)
- [AWSCertificateManagerPrivateCAAuditor](#)
- [AWSCertificateManagerPrivateCAFullAccess](#)
- [AWSCertificateManagerPrivateCAPrivilegedUser](#)
- [AWSCertificateManagerPrivateCARedOnly](#)
- [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](#)
- [Connecteur 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](#)

- [AWSDepRacerRoboMakerAccessPolicy](#)
- [AWSDepRacerServiceRolePolicy](#)
- [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](#)
- [AWSElasticBeanstalkEKSIImageBuild](#)
- [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](#)
- [AWSLambdaVPCLAccessExecutionRole](#)
- [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](#)
- [AWSPCSCComputeNodePolicy](#)
- [AWSPCSServiceRolePolicy](#)
- [AWSPriceListServiceFullAccess](#)
- [AWSPprivateCAAuditor](#)
- [AWSPprivateCAConnectorForKubernetesPolicy](#)
- [AWSPprivateCAFullAccess](#)
- [AWSPprivateCAPrivilegedUser](#)
- [AWSPprivateCARedOnly](#)
- [AWSPprivateCAUser](#)
- [AWSPprivateMarketplaceAdminFullAccess](#)
- [AWSPprivateMarketplaceRequests](#)
- [AWSPprivateNetworksServiceRolePolicy](#)
- [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](#)
- [AWSResilienceHubAssessmentExecutionPolicy](#)
- [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](#)
- [AWSecretsManagerClientReadOnlyAccess](#)
- [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](#)
- [AWSSStepFunctionsConsoleFullAccess](#)
- [AWSSStepFunctionsFullAccess](#)

- [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](#)
- [Facturation](#)
- [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](#)
- [ROSAKMSPProviderPolicy](#)
- [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

Description : Autoriser Access Analyzer à analyser les métadonnées des ressources

AccessAnalyzerServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 02 décembre 2019, 17:13 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

Version de la politique

Version de la politique : v23 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AccountAccessManagerServiceRolePolicy

Description : accorde au gestionnaire d'accès au compte les autorisations nécessaires pour gérer Compte AWS l'accès

AccountAccessManagerServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 29 juin 2026, 19:12 UTC
- Heure modifiée : 29 juin 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccountAccessManagerServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
      }
    }
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AccountManagementFromVercel

Description : À utiliser avec les comptes créés via l'intégration de Vercel Marketplace avec AWS. Permet d'accéder à la gestion des comptes, aux notifications, à l'analyse des coûts et de l'utilisation et à la gestion des fournisseurs d'identité.

AccountManagementFromVercel est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AccountManagementFromVercel à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 décembre 2025, 16:34 UTC
- Heure modifiée : 07 mai 2026, 18:57 UTC
- ARN: arn:aws:iam::aws:policy/AccountManagementFromVercel

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
      }
    }
  ]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AdministratorAccess

Description : Fournit un accès complet aux AWS services et aux ressources.

AdministratorAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AdministratorAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:39 UTC
- Heure modifiée : 06 février 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AdministratorAccess-Amplify

Description : accorde des autorisations administratives au compte tout en autorisant explicitement l'accès direct aux ressources nécessaires aux applications Amplify.

AdministratorAccess-Amplify est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AdministratorAccess-Amplify à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2020, 19:03 UTC
- Heure modifiée : 04 avril 2024, 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-Amplify`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AdministratorAccess-AWSElasticBeanstalk

Description : octroie des autorisations administratives au compte. Permet explicitement aux développeurs et aux administrateurs d'accéder directement aux ressources dont ils ont besoin pour gérer les applications AWS Elastic Beanstalk

AdministratorAccess-AWSElasticBeanstalk est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AdministratorAccess-AWSElasticBeanstalk à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 janvier 2021, 19:36 UTC
- Heure modifiée : 19 mai 2026, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ]
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AgentRegistryFullAccess

Description : fournit un accès complet au registre des AWS agents

AgentRegistryFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AgentRegistryFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 août 2026, 18:12 UTC
- Heure modifiée : 31 août 2026, 17:07 UTC
- ARN: arn:aws:iam::aws:policy/AgentRegistryFullAccess

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "AgentRegistryKMSEncryptKeyForSynchronization",
    "Effect" : "Allow",
    "Action" : [
        "kms:Encrypt"
    ],
    "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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AgentRegistryReadOnlyAccess

Description : Politique d' ReadOnly accès au registre des AWS agents

AgentRegistryReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AgentRegistryReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 août 2026, 18:12 UTC
- Heure modifiée : 06 août 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/AgentRegistryReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*:*:*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AIDevOpsAgentAccessPolicy

Description : fournit les autorisations requises par l' AWS DevOps agent pour mener des enquêtes et effectuer des analyses sur les AWS ressources des clients.

AIDevOpsAgentAccessPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AIDevOpsAgentAccessPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 mars 2026, 03:42 UTC
- Heure modifiée : 24 septembre 2026, 20:57 UTC
- ARN: arn:aws:iam::aws:policy/AIDevOpsAgentAccessPolicy

Version de la politique

Version de la politique : v11 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:GetFirmwareTask",
"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/*/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/"
            ]
        }
    }
}
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège

AIDevOpsAgentActionsPolicy

Description : fournit les autorisations élevées requises par l' AWS DevOps agent pour effectuer des mutations approuvées par l'opérateur ou des actions élevées sur les AWS ressources du client lors d'événements opérationnels.

AIDevOpsAgentActionsPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AIDevOpsAgentActionsPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 juin 2026, 22:27 UTC
- Heure modifiée : 19 août 2026, 22:47 UTC
- ARN: `arn:aws:iam::aws:policy/AIDevOpsAgentActionsPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AIDevOpsAgentFullAccess

Description : fournit un accès complet à Amazon DevOps Agent via le Console de gestion AWS

AIDevOpsAgentFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AIDevOpsAgentFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 mars 2026, 03:42 UTC
- Heure modifiée : 26 juin 2026, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/AIDevOpsAgentFullAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AIDevOpsAgentReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon DevOps Agent via Console de gestion AWS

AIDevOpsAgentReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AIDevOpsAgentReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 mars 2026, 03:42 UTC
- Heure modifiée : 11 juin 2026, 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/AIDevOpsAgentReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AIDevOpsChannelAccessPolicy

Description : Donnez accès au chat et gérez les enquêtes via AWS DevOps Agent pour votre AgentSpaces

AIDevOpsChannelAccessPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AIDevOpsChannelAccessPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 26 août 2026, 21:07 UTC
- Heure modifiée : 26 août 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AIDevOpsChannelAccessPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AIDevOpsConstellationAccessPolicy

Description : fournit les autorisations requises par l' AWS DevOps agent pour assurer la coordination avec les AgentSpaces connexions via la constellation spatiale de l'agent.

AIDevOpsConstellationAccessPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AIDevOpsConstellationAccessPolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 05 août 2026, 16:27 UTC
- Heure modifiée : 05 août 2026, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AIDevOpsConstellationAccessPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AIDevOpsOperatorAppAccessPolicy

Description : Permet d'utiliser l'application Web de AWS DevOps l'opérateur pour un espace d'agent.

AIDevOpsOperatorAppAccessPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AIDevOpsOperatorAppAccessPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 mars 2026, 03:42 UTC
- Heure modifiée : 10 septembre 2026, 17:47 UTC
- ARN: arn:aws:iam::aws:policy/AIDevOpsOperatorAppAccessPolicy

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
    }
}

```

```
}  
  }  
    }  
      ]  
    }  
  }
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AIDevOpsReleaseManagementVPCPolicy

Description : autorise l' AWS DevOps agent à créer et à gérer des interfaces réseau dans votre VPC afin que les agents de gestion des versions puissent accéder à des ressources privées

AIDevOpsReleaseManagementVPCPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AIDevOpsReleaseManagementVPCPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 21 août 2026, 22:27 UTC
- Heure modifiée : 21 août 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/AIDevOpsReleaseManagementVPCPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AIOpsAssistantIncidentReportPolicy

Description : fournit les autorisations requises par l'assistant Amazon AI Operations pour générer un rapport d'incident relatif à l'enquête.

AIOpsAssistantIncidentReportPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AIOpsAssistantIncidentReportPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 10 octobre 2025, 22:04 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsAssistantIncidentReportPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        ]
      }
    }
  }
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AIOpsAssistantPolicy

Description : fournit ReadOnly les autorisations requises par l'assistant Amazon AI Operations pour analyser les AWS ressources des clients lors des enquêtes.

AIOpsAssistantPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AI0psAssistantPolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 décembre 2024, 16:21 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AI0psAssistantPolicy`

Version de la politique

Version de la politique : v15 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AI0PSServiceAccess",
      "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:ListGroup",
"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:GetEntityTypeTypes",
"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*",
"qlldb:Describe*",
"qlldb: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/*"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AI0psConsoleAdminPolicy

Description : accorde un accès complet au service Amazon AI Operations et à ses autorisations requises via AWS la console. Elle inclut également des autorisations pour utiliser des sessions de console sensibles à l'identité.

AI0psConsoleAdminPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AI0psConsoleAdminPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 décembre 2024, 23:51 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AI0psConsoleAdminPolicy`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "CreateAI0psCrossAccountAssistantPolicy",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreatePolicy"
    ],
    "Resource" : "arn:aws:iam:*:*:policy/AI0psCrossAccountAssistantPolicy*"
  },
  {
    "Sid" : "AmazonQAccess",
    "Effect" : "Allow",
    "Action" : [
      "q:StartConversation",
      "q:SendMessage",
      "q:GetConversation",
      "q:ListConversations",
      "q:UpdateConversation",
      "q>DeleteConversation",
      "q:PassRequest"
    ],
    "Resource" : "*"
  }
}
```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AI0psOperatorAccess

Description : donne accès aux API Amazon AI Operations pour créer, mettre à jour et supprimer des enquêtes, des événements d'investigation et des ressources d'investigation. Il inclut également ReadOnly l'accès à toutes les API d'opérations d'IA et l'utilisation de sessions sensibles à l'identité.

AI0psOperatorAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AI0psOperatorAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 décembre 2024, 23:51 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AI0psOperatorAccess`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AI0psOperatorAccess",
      "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" : "*"
    }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AIOpsReadOnlyAccess

Description : accorde des ReadOnly autorisations au service Amazon AI Operations et à ses ressources requises.

AIOpsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AIOpsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 décembre 2024, 23:51 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsReadOnlyAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AlexaForBusinessDeviceSetup

Description : Permettre à la configuration de l'appareil d'accéder aux AlexaForBusiness services

AlexaForBusinessDeviceSetup est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AlexaForBusinessDeviceSetup à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 novembre 2017, 16:47 UTC
- Heure modifiée : 20 mai 2019, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AlexaForBusinessFullAccess

Description : Donne un accès complet aux AlexaForBusiness ressources et à des ressources connexes Services AWS

AlexaForBusinessFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AlexaForBusinessFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 novembre 2017, 16:47 UTC
- Heure modifiée : 01 juillet 2020, 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessFullAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
      }
    }
  }
}

```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AlexaForBusinessGatewayExecution

Description : Fournir un accès aux AlexaForBusiness services pour l'exécution de la passerelle

AlexaForBusinessGatewayExecution est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AlexaForBusinessGatewayExecution à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 novembre 2017, 16:47 UTC
- Heure modifiée : 30 novembre 2017, 16:47 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AlexaForBusinessLifesizeDelegatedAccessPolicy

Description : Permettre l'accès aux appareils Lifesize AVS

AlexaForBusinessLifesizeDelegatedAccessPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AlexaForBusinessLifesizeDelegatedAccessPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 juin 2020, 19:46 UTC
- Heure modifiée : 12 juin 2020, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessLifesizeDelegatedAccessPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*/*:A2IW07UEGWV4TL"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "a4b:RegisterAVSDevice"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "StringEquals" : {
            "a4b:amazonId" : [
                "A2IW07UEGWV4TL"
            ]
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "a4b:SearchDevices"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "ForAllValues:StringLike" : {
            "a4b:filters_deviceType" : [
                "*A2IW07UEGWV4TL"
            ]
        },
        "Null" : {
            "a4b:filters_deviceType" : "false"
        }
    }
},

```

```

{
  "Effect" : "Allow",
  "Action" : [
    "a4b:AssociateDeviceWithRoom"
  ],
  "Resource" : [
    "arn:aws:a4b:us-east-1:*:device/*/*:A2IW07UEGWV4TL",
    "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/*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AlexaForBusinessNetworkProfileServicePolicy

Description : Cette politique permet à Alexa for Business d'effectuer des tâches automatisées planifiées par vos profils réseau.

AlexaForBusinessNetworkProfileServicePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 13 mars 2019, 00:53 UTC
- Heure modifiée : 05 avril 2019, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AlexaForBusinessPolyDelegatedAccessPolicy

Description : Fournir un accès aux appareils Poly AVS

AlexaForBusinessPolyDelegatedAccessPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AlexaForBusinessPolyDelegatedAccessPolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 16 octobre 2019, 19:48 UTC
- Heure modifiée : 16 octobre 2019, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AlexaForBusinessReadOnlyAccess

Description : Fournir un accès en lecture seule aux AlexaForBusiness services

AlexaForBusinessReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AlexaForBusinessReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 novembre 2017, 16:47 UTC
- Heure modifiée : 20 novembre 2019, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonAPIGatewayAdministrator

Description : fournit un accès complet aux API create/edit /delete dans Amazon API Gateway via le Console de gestion AWS.

AmazonAPIGatewayAdministrator est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonAPIGatewayAdministrator à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 juillet 2015, 17:34 UTC
- Heure modifiée : 09 juillet 2015, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonAPIGatewayInvokeFullAccess

Description : fournit un accès complet pour invoquer des API dans Amazon API Gateway.

AmazonAPIGatewayInvokeFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonAPIGatewayInvokeFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 juillet 2015, 17:36 UTC
- Heure modifiée : 18 décembre 2018, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "execute-api:ManageConnections"
      ],
      "Resource" : "arn:aws:execute-api:*:*:*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonAPIGatewayPushToCloudWatchLogs

Description : permet à API Gateway de transférer les journaux vers le compte de l'utilisateur.

AmazonAPIGatewayPushToCloudWatchLog est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonAPIGatewayPushToCloudWatchLogs à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 11 novembre 2015, 23:41 UTC
- Heure modifiée : 11 novembre 2015, 23:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonAppFlowFullAccess

Description : fournit un accès complet à Amazon AppFlow et aux AWS services pris en charge en tant que source ou destination de flux (S3 et Redshift). Fournit également un accès à KMS pour le chiffrement

AmazonAppFlowFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonAppFlowFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 02 juin 2020, 23:30 UTC
- Heure modifiée : 28 février 2022, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]

```



```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonAppFlowReadOnlyAccess

Description : fournit un accès en lecture seule aux flux Amazon Appflow

AmazonAppFlowReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonAppFlowReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 juin 2020, 23:26 UTC
- Heure modifiée : 28 février 2022, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy

Description : accorde des autorisations au commutateur de région ARC pour l'exécution et l'évaluation du plan.

AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer

AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 novembre 2025, 19:34 UTC
- Heure modifiée : 02 octobre 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonAppStreamFullAccess

Description : fournit un accès complet à Amazon AppStream via le Console de gestion AWS.

AmazonAppStreamFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonAppStreamFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 28 août 2020, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamFullAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonAppStreamPCAAccess

Description : Accès Amazon AppStream 2.0 à AWS Certificate Manager Private CA dans les comptes clients pour l'authentification basée sur les certificats

AmazonAppStreamPCAAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonAppStreamPCAAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 24 octobre 2022, 17:05 UTC
- Heure modifiée : 24 octobre 2022, 17:05 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonAppStreamReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon AppStream via le Console de gestion AWS.

AmazonAppStreamReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonAppStreamReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamReadOnlyAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonAppStreamServiceAccess

Description : Politique par défaut pour le rôle AppStream de service Amazon.

AmazonAppStreamServiceAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonAppStreamServiceAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 19 novembre 2016, 04:17 UTC
- Heure modifiée : 03 septembre 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonAthenaFullAccess

Description : Fournissez un accès complet à Amazon Athena et un accès limité aux dépendances nécessaires pour permettre les requêtes, l'écriture des résultats et la gestion des données.

AmazonAthenaFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonAthenaFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 novembre 2016, 16:46 UTC
- Heure modifiée : 12 février 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAthenaFullAccess`

Version de la politique

Version de la politique : v15 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "*"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonAthenaServiceRolePolicy

Description : Permet d'accéder à d'autres ressources de AWS service requises pour exécuter Amazon Athena

AmazonAthenaServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 14 novembre 2025, 22:34 UTC
- Heure modifiée : 14 novembre 2025, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonAthenaServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonAugmentedAIFullAccess

Description : Permet d'effectuer toutes les opérations sur les ressources Amazon Augmented AI FlowDefinitions, y compris HumanTaskUis et HumanLoops. N'autorise pas l'accès à l'équipe de travail créée FlowDefinitions contre la foule.

AmazonAugmentedAIFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonAugmentedAIFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 décembre 2019, 16:21 UTC
- Heure modifiée : 3 décembre 2019, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      ]
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonAugmentedAIHumanLoopFullAccess

Description : Permet d'effectuer toutes les opérations sur HumanLoops.

AmazonAugmentedAIHumanLoopFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonAugmentedAIHumanLoopFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 décembre 2019, 16:20 UTC
- Heure modifiée : 03 décembre 2019, 16:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonAugmentedAIIntegratedAPIAccess

Description : Permet d'effectuer toutes les opérations sur les ressources Amazon Augmented AI FlowDefinitions, y compris HumanTaskUis et HumanLoops. Permet également d'accéder aux opérations des services intégrés à Amazon Augmented AI.

AmazonAugmentedAIIntegratedAPIAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonAugmentedAIIntegratedAPIAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 avril 2020, 20:47 UTC
- Heure modifiée : 22 avril 2020, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            ]
        }
    }
}

```

```
}  
  }  
    }  
      ]  
    }  
  }
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonAuroraDSQLConsoleFullAccess

Description : fournit à la console un accès administratif complet à Aurora DSQL

AmazonAuroraDSQLConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonAuroraDSQLConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 décembre 2024, 15:36 UTC
- Heure modifiée : 13 mai 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLConsoleFullAccess`

Version de la politique

Version de la politique : v16 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
                "dsq1.*.amazonaws.com"
            ]
        },
        "ForAnyValue:StringEquals" : {
            "kms:EncryptionContextKeys" : "aws:dsq1: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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonAuroraDSQLEFullAccess

Description : fournit un accès administratif complet à Aurora DSQL

AmazonAuroraDSQLEFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonAuroraDSQLEFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 décembre 2024, 15:36 UTC

- Heure modifiée : 13 mai 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLFullAccess`

Version de la politique

Version de la politique : v16 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "dsq1.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KMSCryptographicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsq1.*.amazonaws.com"
          ]
        }
      },
      "ForAnyValue:StringEquals" : {
        "kms:EncryptionContextKeys" : "aws:dsq1:ClusterId"
      }
    }
  ]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonAuroraDSQLReadOnlyAccess

Description : fournit un accès en lecture seule à Aurora DSQL

AmazonAuroraDSQLReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonAuroraDSQLReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 décembre 2024, 15:21 UTC
- Heure modifiée : 13 mai 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLReadOnlyAccess`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRole

Description : fournit l'autorisation d'inférer le modèle Bedrock à la mémoire centrale de l'agent Bedrock

AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer

AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 16 juillet 2025, 13:37 UTC
- Heure modifiée : 17 juillet 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonBedrockExternalWebSearchFullAccess

Description : fournit un accès complet à Amazon Bedrock Web Search, y compris la récupération de contenu à partir de sites Web externes situés en dehors des limites du AWS réseau.

AmazonBedrockExternalWebSearchFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonBedrockExternalWebSearchFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 03 août 2026, 16:57 UTC
- Heure modifiée : 03 août 2026, 16:57 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBedrockExternalWebSearchFullAccess

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*:*:*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonBedrockExternalWebSearchReadOnly

Description : fournit un accès en lecture seule à Amazon Bedrock Web Search, y compris la récupération de contenu à partir de sites Web externes situés en dehors des limites du réseau. AWS

AmazonBedrockExternalWebSearchReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonBedrockExternalWebSearchReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 août 2026, 16:57 UTC
- Heure modifiée : 03 août 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockExternalWebSearchReadOnly`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*:*:*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonBedrockFullAccess

Description : fournit un accès complet à Amazon Bedrock ainsi qu'un accès limité aux services connexes requis par celui-ci

AmazonBedrockFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonBedrockFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 décembre 2023, 15:47 UTC
- Heure modifiée : 04 août 2026, 05:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBedrockFullAccess

Version de la politique

Version de la politique : v11 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonBedrockLimitedAccess

Description : fournit un accès limité à Amazon Bedrock ainsi qu'aux services associés requis par celui-ci

AmazonBedrockLimitedAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonBedrockLimitedAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 29 juin 2025, 22:22 UTC
- Heure modifiée : 04 août 2026, 05:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockLimitedAccess`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonBedrockMantleFullAccess

Description : Fournit un accès complet à Amazon Bedrock Mantle ainsi qu'un accès limité aux services connexes requis par celui-ci

AmazonBedrockMantleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonBedrockMantleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 décembre 2025, 07:19 UTC
- Heure modifiée : 04 août 2026, 04:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMantleFullAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonBedrockMantleInferenceAccess

Description : permet d'accéder à la lecture et à la création d'inférences à Amazon Bedrock Mantle

AmazonBedrockMantleInferenceAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonBedrockMantleInferenceAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 décembre 2025, 07:19 UTC
- Heure modifiée : 04 août 2026, 05:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMantleInferenceAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonBedrockMantleReadOnly

Description : fournit un accès en lecture seule à Amazon Bedrock Mantle

AmazonBedrockMantleReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonBedrockMantleReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 décembre 2025, 07:19 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMantleReadOnly`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonBedrockMarketplaceAccess

Description : fournit un accès limité à Amazon Bedrock Marketplace ainsi qu'aux services associés requis par celui-ci

AmazonBedrockMarketplaceAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonBedrockMarketplaceAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 juin 2025, 22:22 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMarketplaceAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ]
  }
}
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonBedrockReadOnly

Description : fournit un accès en lecture seule à Amazon Bedrock

AmazonBedrockReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonBedrockReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 décembre 2023, 15:48 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonBedrockReadOnly`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonBedrockStudioPermissionsBoundary

Description : définit les autorisations maximales des rôles IAM créés par Amazon Bedrock Studio pour l'exploitation des ressources Amazon Bedrock Studio.

AmazonBedrockStudioPermissionsBoundary est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonBedrockStudioPermissionsBoundary` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 août 2024, 00:24 UTC
- Heure modifiée : 01 août 2024, 00:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockStudioPermissionsBoundary`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      ]
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonBedrockWebSearchFullAccess

Description : fournit un accès complet à Amazon Bedrock Web Search. Les données restent dans les limites AWS du réseau.

AmazonBedrockWebSearchFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonBedrockWebSearchFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 août 2026, 16:42 UTC
- Heure modifiée : 03 août 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockWebSearchFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonBedrockWebSearchReadOnly

Description : fournit un accès en lecture seule à Amazon Bedrock Web Search. Les données restent dans les limites AWS du réseau.

AmazonBedrockWebSearchReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonBedrockWebSearchReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 août 2026, 16:57 UTC
- Heure modifiée : 03 août 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockWebSearchReadOnly`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
"Effect" : "Allow",
"Action" : [
    "bedrock-websearch:InvokeSearch",
    "bedrock-websearch:InvokeFetch"
],
"Resource" : "arn:aws:bedrock-websearch:*:*:*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonBioDiscoveryFullAccess

Description : Permet un accès administratif complet à Amazon Bio Discovery

AmazonBioDiscoveryFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonBioDiscoveryFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 août 2026, 06:27 UTC
- Heure modifiée : 18 août 2026, 06:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBioDiscoveryFullAccess

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonBioDiscoveryInAppFullAccess

Description : fournit un accès complet aux actions des applications Amazon Bio Discovery

AmazonBioDiscoveryInAppFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonBioDiscoveryInAppFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 août 2026, 06:47 UTC
- Heure modifiée : 18 août 2026, 06:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBioDiscoveryInAppFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonBraketFullAccess

Description : fournit un accès complet à Amazon Braket via le SDK Console de gestion AWS et. Permet également d'accéder à des services connexes (par exemple, S3, journaux).

AmazonBraketFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonBraketFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 août 2020, 20:12 UTC
- Heure modifiée : 06 juillet 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketFullAccess`

Version de la politique

Version de la politique : v13 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonBraketJobsExecutionPolicy

Description : accorde l'accès Services AWS et les ressources nécessaires à l'exécution d'un job Amazon Braket, notamment S3, Cloudwatch, IAM et Braket

AmazonBraketJobsExecutionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonBraketJobsExecutionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 novembre 2021, 19:34 UTC
- Heure modifiée : 06 juillet 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonBraketServiceRolePolicy

Description : Permet à Amazon Braket de créer et de gérer des AWS ressources en votre nom

AmazonBraketServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 04 août 2020, 17:12 UTC
- Heure modifiée : 06 juillet 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
    }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonChimeFullAccess

Description : fournit un accès complet à la console d'administration Amazon Chime via le Console de gestion AWS.

AmazonChimeFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonChimeFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 novembre 2017, 22:15 UTC
- Heure modifiée : 14 décembre 2020, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ],
    "Resource" : [
        "arn:aws:kinesis:*:*:ChimeVoiceConnector-Streaming*"
    ]
}
```

```
    "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-*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonChimeReadOnly

Description : fournit un accès en lecture seule à la console d'administration Amazon Chime via le Console de gestion AWS.

AmazonChimeReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonChimeReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 novembre 2017, 22:04 UTC
- Heure modifiée : 14 décembre 2020, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeReadOnly`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonChimeSDK

Description : Permet d'accéder aux opérations du SDK Amazon Chime

AmazonChimeSDK est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonChimeSDK à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 février 2020, 21:53 UTC
- Heure modifiée : 10 janvier 2023, 18:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeSDK`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

Description : Politique gérée pour le rôle lié au MediaPipelines service Amazon Chime SDK

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 04 avril 2022, 22:02 UTC
- Heure modifiée : 08 décembre 2023, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]

```

```
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonChimeSDKMessagingServiceRolePolicy

Description : Permet à Amazon Chime SDK Messaging d'accéder aux AWS ressources et d'activer la fonctionnalité de messagerie

AmazonChimeSDKMessagingServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 03 mars 2023, 01:43 UTC
- Heure modifiée : 03 mars 2023, 01:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
    ]
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonChimeServiceRolePolicy

Description : Permet d'accéder aux AWS ressources utilisées ou gérées par Amazon Chime

AmazonChimeServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 30 septembre 2019, 22:25 UTC
- Heure modifiée : 30 septembre 2019, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

```
}  
}  
]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonChimeTranscriptionServiceLinkedRolePolicy

Description : permet à Amazon Chime d'accéder à Amazon Transcribe et Amazon Transcribe Medical en votre nom

AmazonChimeTranscriptionServiceLinkedRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 04 août 2021, 21:47 UTC
- Heure modifiée : 04 août 2021, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeTranscriptionServiceLinkedRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonChimeUserManagement

Description : Fournit un accès de gestion des utilisateurs à la console d'administration Amazon Chime via le Console de gestion AWS.

AmazonChimeUserManagement est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonChimeUserManagement à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 novembre 2017, 22:17 UTC
- Heure modifiée : 18 février 2020, 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeUserManagement`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

Description : Politique gérée pour le rôle lié à un service pour Amazon Chime VoiceConnector

AmazonChimeVoiceConnectorServiceLinkedRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 30 septembre 2019, 22:16 UTC

- Heure modifiée : 14 avril 2023, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
      "*"
    ]
  }
}
```

```
]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCloudDirectoryFullAccess

Description : fournit un accès complet à Amazon Cloud Directory Service.

AmazonCloudDirectoryFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonCloudDirectoryFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 février 2017, 00:41 UTC
- Heure modifiée : 25 février 2017, 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCloudDirectoryReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon Cloud Directory Service.

AmazonCloudDirectoryReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonCloudDirectoryReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 février 2017, 23:42 UTC
- Heure modifiée : 28 février 2017, 23:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCloudWatchEvidentlyFullAccess

Description : fournit un accès complet uniquement à Amazon CloudWatch Evidently. Permet également d'accéder à Amazon S3, Amazon SNS CloudWatch, Amazon et à d'autres services connexes.

AmazonCloudWatchEvidentlyFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonCloudWatchEvidentlyFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2021, 15:10 UTC
- Heure modifiée : 29 novembre 2021, 15:10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
```

```
        "*"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCloudWatchEvidentlyReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon CloudWatch Evidently

AmazonCloudWatchEvidentlyReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonCloudWatchEvidentlyReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2021, 15:08 UTC
- Heure modifiée : 29 novembre 2021, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCloudWatchEvidentlyServiceRolePolicy

Description : Permet à CloudWatch Evidently Service de gérer les AWS ressources associées pour le compte du client

AmazonCloudWatchEvidentlyServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 13 septembre 2022, 17:25 UTC
- Heure modifiée : 13 septembre 2022, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCloudWatchRUMFullAccess

Description : accorde des autorisations d'accès complètes au service Amazon CloudWatch RUM

AmazonCloudWatchRUMFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonCloudWatchRUMFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2021, 15:46 UTC
- Heure modifiée : 29 novembre 2021, 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCloudWatchRUMReadOnlyAccess

Description : accorde des autorisations en lecture seule pour le service Amazon CloudWatch RUM

AmazonCloudWatchRUMReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonCloudWatchRUMReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2021, 15:43 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCloudWatchRUMServiceRolePolicy

Description : autorise Amazon CloudWatch RUM Service à publier des données de surveillance pour d'autres AWS services concernés

AmazonCloudWatchRUMServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle

- Heure de création : 17 novembre 2021, 23:17 UTC
- Heure modifiée : 22 février 2023, 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
          ]
        }
      }
    }
  ]
}
```

```
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCodeCatalystFullAccess

Description : fournit un accès complet à Amazon CodeCatalyst

AmazonCodeCatalystFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonCodeCatalystFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 avril 2023, 16:50 UTC
- Heure modifiée : 20 avril 2023, 16:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCodeCatalystReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon CodeCatalyst

AmazonCodeCatalystReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonCodeCatalystReadOnlyAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 avril 2023, 16:49 UTC
- Heure modifiée : 20 avril 2023, 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCodeCatalystSupportAccess

Description : permet CodeCatalyst à Amazon de créer, de mettre à jour et de résoudre AWS Support des requêtes en votre nom.

AmazonCodeCatalystSupportAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonCodeCatalystSupportAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 20 avril 2023, 12:34 UTC
- Heure modifiée : 20 avril 2023, 12:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCodeGuruProfilerAgentAccess

Description : fournit l'accès requis par l'agent Amazon CodeGuru Profiler.

AmazonCodeGuruProfilerAgentAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonCodeGuruProfilerAgentAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 février 2021, 22:11 UTC
- Heure modifiée : 05 mai 2022, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:ConfigureAgent",
        "codeguru-profiler:CreateProfilingGroup",
        "codeguru-profiler:PostAgentProfile"
      ],
      "Resource" : "arn:aws:codeguru-profiler:*:*:profilingGroup/*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCodeGuruProfilerFullAccess

Description : fournit un accès complet à Amazon CodeGuru Profiler.

AmazonCodeGuruProfilerFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonCodeGuruProfilerFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 décembre 2019, 10:13 UTC
- Heure modifiée : 15 juillet 2020, 03:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCodeGuruProfilerReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon CodeGuru Profiler.

AmazonCodeGuruProfilerReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonCodeGuruProfilerReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 03 décembre 2019, 10:30 UTC
- Heure modifiée : 27 juin 2020, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCodeGuruReviewerFullAccess

Description : accorde un accès complet à Amazon CodeGuru Reviewer et un accès limité aux dépendances requises.

AmazonCodeGuruReviewerFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonCodeGuruReviewerFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 décembre 2019, 08:33 UTC
- Heure modifiée : 29 août 2020, 04:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"  
    }  
  }  
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCodeGuruReviewerReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon CodeGuru Reviewer.

AmazonCodeGuruReviewerReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonCodeGuruReviewerReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 décembre 2019, 08:48 UTC
- Heure modifiée : 29 août 2020, 04:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruReviewerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru:Get*",
        "codeguru-reviewer:List*",
        "codeguru-reviewer:Describe*",
        "codeguru-reviewer:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCodeGuruReviewerServiceRolePolicy

Description : rôle lié à un service requis pour qu'Amazon CodeGuru Reviewer puisse accéder aux ressources en votre nom.

AmazonCodeGuruReviewerServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 03 décembre 2019, 05:31 UTC
- Heure modifiée : 27 novembre 2020, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*/*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCodeGuruSecurityFullAccess

Description : fournit un accès complet à Amazon CodeGuru Security.

AmazonCodeGuruSecurityFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonCodeGuruSecurityFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 mai 2023, 21:03 UTC

- Heure modifiée : 09 mai 2023, 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCodeGuruSecurityScanAccess

Description : fournit l'accès requis pour utiliser les scans Amazon CodeGuru Security.

AmazonCodeGuruSecurityScanAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonCodeGuruSecurityScanAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 mai 2023, 20:54 UTC
- Heure modifiée : 09 mai 2023, 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    }
  ]
}
```


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCognitoDeveloperAuthenticatedIdentities

Description : donne accès aux API Amazon Cognito pour prendre en charge les identités authentifiées des développeurs à partir de votre backend d'authentification.

AmazonCognitoDeveloperAuthenticatedIdentities est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonCognitoDeveloperAuthenticatedIdentities à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 mars 2015, 17:22 UTC
- Heure modifiée : 24 mars 2015, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoDeveloperAuthenticatedIdentities`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:GetOpenIdTokenForDeveloperIdentity",
        "cognito-identity:LookupDeveloperIdentity",
        "cognito-identity:MergeDeveloperIdentities",
        "cognito-identity:UnlinkDeveloperIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCognitoIdpEmailServiceRolePolicy

Description : Permet au service Amazon Cognito User Pools d'utiliser vos identités SES pour l'envoi d'e-mails

AmazonCognitoIdpEmailServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 21 mars 2019, 21:32 UTC
- Heure modifiée : 21 mars 2019, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ses:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCognitoIdpServiceRolePolicy

Description : Permet l'accès aux groupes d'utilisateurs Amazon Cognito Services AWS et aux ressources utilisées ou gérées par ceux-ci

AmazonCognitoIdpServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 26 juin 2020, 22:30 UTC
- Heure modifiée : 26 juin 2020, 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
```

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCognitoPowerUser

Description : fournit un accès administratif aux ressources Amazon Cognito existantes. Vous aurez besoin de privilèges Compte AWS d'administrateur pour créer de nouvelles ressources Cognito.

AmazonCognitoPowerUser est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonCognitoPowerUser à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 mars 2015, 17:14 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoPowerUser

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCognitoReadOnly

Description : fournit un accès en lecture seule aux ressources Amazon Cognito.

AmazonCognitoReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonCognitoReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 24 mars 2015, 17:06 UTC
- Heure modifiée : 01 août 2019, 19:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoReadOnly

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCognitoUnAuthedIdentitiesSessionPolicy

Description : Cette politique définit l'ensemble des autorisations autorisées pour les identités non authentifiées pour les pools d'identités Cognito. Cette politique n'est pas destinée à être utilisée comme une politique d'autorisation autonome. Il est utilisé comme un garde-fou contre les politiques trop permissives associées aux rôles dans un pool d'identités. N'associez cette politique à aucun rôle, car Cognito Identity Service l'inclura automatiquement en tant que politique restreinte lors de la création d'informations d'identification. Les privilèges permettant d'accéder temporairement à d'autres AWS ressources via le flux amélioré seront désormais définis à l'intersection du rôle associé à l'identité de l'utilisateur non authentifié fourni par un service et des privilèges accordés dans cette politique gérée qui appartient à Cognito.

AmazonCognitoUnAuthedIdentitiesSessionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonCognitoUnAuthedIdentitiesSessionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- **Type** : politique AWS gérée
- **Heure de création** : 19 juillet 2023, 23:04 UTC
- **Heure modifiée** : 01 mai 2026, 19:57 UTC
- **ARN**: arn:aws:iam::aws:policy/AmazonCognitoUnAuthedIdentitiesSessionPolicy

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CognitoUnAuthenticatedSessionPolicy",
      "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" : "*"
    }
  ]
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonCognitoUnauthenticatedIdentities

Description : Cette politique définit l'ensemble des autorisations autorisées pour les identités non authentifiées pour les pools d'identités Cognito. Cela n'a pas besoin d'être associé à votre rôle d'authentification, car Cognito Identity Service l'inclura automatiquement en tant que politique restreinte lors de la création d'informations d'identification. Les privilèges permettant d'accéder temporairement à d'autres AWS ressources via le flux amélioré seront désormais définis à l'intersection du rôle associé à l'identité de l'utilisateur non authentifié fourni par un service et des privilèges accordés dans cette politique gérée qui appartient à Cognito.

AmazonCognitoUnauthenticatedIdentities est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonCognitoUnauthenticatedIdentities à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 février 2023, 22:36 UTC
- Heure modifiée : 01 février 2023, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonConnect_FullAccess

Description : Le but de cette politique est d'accorder les autorisations nécessaires aux utilisateurs AWS Connect pour utiliser les ressources Connect. Cette politique fournit un accès complet aux ressources AWS Connect via la console Connect et les API publiques

AmazonConnect_FullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonConnect_FullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 20 novembre 2020, 19:54 UTC
- Heure modifiée : 07 mars 2023, 14:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnect_FullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonConnectCampaignsServiceLinkedRolePolicy

Description : Politique relative au rôle lié au service Amazon Connect Campaigns

AmazonConnectCampaignsServiceLinkedRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 23 septembre 2021, 20:54 UTC
- Heure modifiée : 18 juin 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectCampaignsServiceLinkedRolePolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonConnectReadOnlyAccess

Description : accorde l'autorisation d'afficher les instances Amazon Connect de votre Compte AWS.

AmazonConnectReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonConnectReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 octobre 2018, 21:00 UTC
- Heure modifiée : 19 juin 2024, 15:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonConnectServiceLinkedRolePolicy

Description : permet à Amazon Connect de créer et de gérer AWS des ressources en votre nom.

AmazonConnectServiceLinkedRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 07 septembre 2018, 00:21 UTC
- Heure modifiée : 02 octobre 2026, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy`

Version de la politique

Version de la politique : v56 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-D0-
NOT-DELETE",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid" : "PassRoleToSESToReceiptRuleManagement",
    "Effect" : "Allow",
    "Action" : [
        "iam:PassRole"
    ],
    "Resource" : [
        "arn:aws:iam:*:*:role/service-role/AmazonConnectEmailSESAccessRole"
    ],
    "Condition" : {
        "StringLike" : {
            "iam:PassedToService" : "ses.amazonaws.com"
        }
    }
},
{
    "Sid" : "AllowSocialMessagingOperations",
    "Effect" : "Allow",
    "Action" : [
        "social-messaging:SendWhatsAppMessage",
        "social-messaging:PostWhatsAppMessageMedia",
        "social-messaging:GetWhatsAppMessageMedia",
        "social-messaging:GetLinkedWhatsAppBusinessAccountPhoneNumber",
        "social-messaging:SendWhatsAppCallEvent"
    ],
    "Resource" : "arn:aws:social-messaging:*:*:phone-number-id/*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${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" : [  
        "*"   
    ]  
  }  
]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonConnectSynchronizationServiceRolePolicy

Description : permet à Amazon Connect de synchroniser les AWS ressources entre les régions en votre nom.

AmazonConnectSynchronizationServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 27 octobre 2023, 22:38 UTC
- Heure modifiée : 21 novembre 2025, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonConnectVoiceIDFullAccess

Description : fournit un accès complet à Amazon Connect Voice ID

AmazonConnectVoiceIDFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonConnectVoiceIDFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 septembre 2021, 19:04 UTC
- Heure modifiée : 26 septembre 2021, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDataZoneBedrockModelConsumptionPolicy

Description : fournit les autorisations nécessaires pour utiliser les modèles Amazon Bedrock, notamment en invoquant le profil d'inférence d'application Amazon Bedrock créé pour un domaine Amazon spécifique. DataZone

AmazonDataZoneBedrockModelConsumptionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDataZoneBedrockModelConsumptionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 12 novembre 2024, 22:15 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneBedrockModelConsumptionPolicy`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDataZoneBedrockModelManagementPolicy

Description : fournit les autorisations nécessaires pour gérer l'accès au modèle Amazon Bedrock, notamment pour créer, baliser et supprimer des profils d'inférence d'applications.

AmazonDataZoneBedrockModelManagementPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDataZoneBedrockModelManagementPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 12 novembre 2024, 22:14 UTC
- Heure modifiée : 12 novembre 2024, 22:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneBedrockModelManagementPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDataZoneDomainExecutionRolePolicy

Description : Politique par défaut pour le rôle DataZone de DomainExecutionRole service d'Amazon. Ce rôle est utilisé par Amazon DataZone pour cataloguer, découvrir, gérer, partager et analyser les données du DataZone domaine Amazon.

AmazonDataZoneDomainExecutionRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDataZoneDomainExecutionRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 27 septembre 2023, 21:55 UTC
- Heure modifiée : 26 février 2026, 00:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy`

Version de la politique

Version de la politique : v13 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDataZoneEnvironmentRolePermissionsBoundary

Description : Amazon DataZone crée des rôles IAM pour les environnements afin d'effectuer des actions d'analyse de données, et utilise cette politique lors de la création de ces rôles afin de définir les limites de leurs autorisations.

AmazonDataZoneEnvironmentRolePermissionsBoundary est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDataZoneEnvironmentRolePermissionsBoundary à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 septembre 2023, 23:38 UTC
- Heure modifiée : 17 novembre 2023, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneEnvironmentRolePermissionsBoundary`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "*"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDataZoneFullAccess

Description : Fournit un accès complet à Amazon DataZone via le, Console de gestion AWS ainsi qu'un accès limité aux services connexes requis par celui-ci.

AmazonDataZoneFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDataZoneFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 septembre 2023, 20:06 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullAccess`

Version de la politique

Version de la politique : v13 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDataZoneFullUserAccess

Description : fournit un accès complet à Amazon DataZone, mais n'autorise pas la gestion des domaines, des utilisateurs ou des comptes associés.

AmazonDataZoneFullUserAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDataZoneFullUserAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 septembre 2023, 21:06 UTC
- Heure modifiée : 19 novembre 2024, 21:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDataZoneGlueManageAccessRolePolicy

Description : La politique accorde des autorisations permettant DataZone à Amazon d'activer la publication et d'accéder aux données.

AmazonDataZoneGlueManageAccessRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDataZoneGlueManageAccessRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 22 septembre 2023, 20:21 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneGlueManageAccessRolePolicy`

Version de la politique

Version de la politique : v18 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDataZonePortalFullAccessPolicy

Description : fournit un accès complet aux DataZone API Amazon

AmazonDataZonePortalFullAccessPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDataZonePortalFullAccessPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 mars 2023, 18:24 UTC
- Heure modifiée : 26 mars 2023, 18:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDataZonePreviewConsoleFullAccess

Description : fournit un accès complet à la version préliminaire d'Amazon DataZone via le Console de gestion AWS. Fournit également un accès sélectif à d'autres services connexes.

AmazonDataZonePreviewConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDataZonePreviewConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 mars 2023, 15:16 UTC
- Heure modifiée : 13 juillet 2023, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDataZoneProjectDeploymentPermissionsBoundary

Description : Amazon DataZone crée des rôles IAM qu'il utilise pour déployer des projets d'analyse de données. DataZone utilise cette politique lors de la création de ces rôles afin de définir les limites de leurs autorisations.

AmazonDataZoneProjectDeploymentPermissionsBoundary est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDataZoneProjectDeploymentPermissionsBoundary à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 21 mars 2023, 02:54 UTC
- Heure modifiée : 04 avril 2023, 02:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectDeploymentPermissionsBoundary`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
    "*"
  ]

```

```
]
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDataZoneProjectRolePermissionsBoundary

Description : Amazon DataZone crée des rôles IAM pour les projets afin d'effectuer des actions d'analyse de données, et utilise cette politique lors de la création de ces rôles afin de définir les limites de leurs autorisations.

AmazonDataZoneProjectRolePermissionsBoundary est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDataZoneProjectRolePermissionsBoundary à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 21 mars 2023, 02:51 UTC
- Heure modifiée : 21 mars 2023, 02:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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",
"iam:*",
"redshift:*",
"redshift-data:*",
"tag:GetResources",
"iam:List*",
"iam:GetRole",
"iam:GetRolePolicy",
"iam:PassRole",
```

```
        "sqlworkbench:*",
        "datazone:*"
    ],
    "Resource" : [
        "*"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDataZoneRedshiftGlueProvisioningPolicy

Description : Amazon DataZone est un service de gestion de données qui vous permet de cataloguer, de découvrir, de gérer, de partager et d'analyser vos données. Avec Amazon DataZone, vous pouvez partager vos données et y accéder entre différents comptes et régions prises en charge. Amazon DataZone simplifie votre expérience sur l'ensemble AWS des services, y compris, mais sans s'y limiter, Amazon Redshift, Amazon Athena, AWS Glue et AWS Lake Formation.

AmazonDataZoneRedshiftGlueProvisioningPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDataZoneRedshiftGlueProvisioningPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 septembre 2023, 20:19 UTC
- Heure modifiée : 21 août 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "AmazonDataZoneEnvironmentKMSEncryptPermissions",
    "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*"
        }
      }
    }
  ]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDataZoneRedshiftManageAccessRolePolicy

Description : Cette politique autorise Amazon DataZone à publier des données Amazon Redshift dans le catalogue. Il permet également à Amazon DataZone d'accorder ou de révoquer l'accès aux ressources publiées par Amazon Redshift ou Amazon Redshift Serverless dans le catalogue.

AmazonDataZoneRedshiftManageAccessRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDataZoneRedshiftManageAccessRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 22 septembre 2023, 20:15 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

Description : La AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary politique est la liste des autorisations autorisées sur un rôle d'exécution créé dans un SageMaker environnement fourni par Amazon DataZone.

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundaryest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 avril 2024, 23:01 UTC
- Heure modifiée : 17 juillet 2026, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`

Version de la politique

Version de la politique : v13 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDataZoneSageMakerManageAccessRolePolicy

Description : La AmazonDataZoneSageMakerManageAccessRolePolicy politique accorde à Amazon DataZone les autorisations nécessaires pour accorder aux utilisateurs l'accès aux différentes ressources de l' SageMaker environnement.

AmazonDataZoneSageMakerManageAccessRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDataZoneSageMakerManageAccessRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 23 avril 2024, 23:34 UTC
- Heure modifiée : 12 février 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerManageAccessRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "AmazonSageMakerKMSSGrantPermission",
    "Effect" : "Allow",
    "Action" : [
      "kms:CreateGrant"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:TagKeys" : [
          "AmazonDataZoneEnvironment"
        ]
      },
      "ForAllValues:StringEquals" : {
        "kms:GrantOperations" : [
          "Decrypt"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDataZoneSageMakerProvisioningRolePolicy

Description : La AmazonDataZoneSageMakerProvisioningRolePolicy politique accorde à Amazon DataZone les autorisations nécessaires pour interagir avec Amazon SageMaker.

AmazonDataZoneSageMakerProvisioningRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDataZoneSageMakerProvisioningRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 avril 2024, 23:32 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerProvisioningRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      ]
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDetectiveFullAccess

Description : fournit un accès complet au service Amazon Detective et un accès limité aux dépendances de l'interface utilisateur de la console

AmazonDetectiveFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDetectiveFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 avril 2020, 17:57 UTC
- Heure modifiée : 17 mai 2023, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDetectiveInvestigatorAccess

Description : fournit aux enquêteurs un accès au service Amazon Detective et un accès limité aux dépendances de l'interface utilisateur de la console. Cette politique accorde l'autorisation de plonger dans Detective à des fins d'enquête et un accès écrit limité à Guardduty.

AmazonDetectiveInvestigatorAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDetectiveInvestigatorAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 janvier 2023, 15:24 UTC

- Heure modifiée : 27 novembre 2023, 03:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDetectiveMemberAccess

Description : fournit aux membres un accès au service Amazon Detective et un accès limité aux dépendances de l'interface utilisateur de la console.

AmazonDetectiveMemberAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDetectiveMemberAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 janvier 2023, 15:16 UTC
- Heure modifiée : 17 janvier 2023, 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDetectiveOrganizationsAccess

Description : permet aux organisations d'accéder à la gestion de l'administrateur délégué pour Amazon Detective et d'accéder de manière limitée aux dépendances de l'interface utilisateur de la console. Cela autorise également la création d'un rôle lié à un service pour Detective.

AmazonDetectiveOrganizationsAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDetectiveOrganizationsAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 mars 2023, 15:20 UTC
- Heure modifiée : 02 mars 2023, 15:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDetectiveServiceLinkedRolePolicy

Description : Permet à Amazon Detective de passer des appels de service en votre nom

AmazonDetectiveServiceLinkedRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 18 novembre 2021, 19:47 UTC
- Heure modifiée : 18 novembre 2021, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ]
    }
  ]
}
```

```
    ],  
    "Resource" : "*"br/>  }  
]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDevOpsGuruConsoleFullAccess

Description : La politique accorde un accès complet à la console DevOps Guru.

AmazonDevOpsGuruConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDevOpsGuruConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 décembre 2021, 18:43 UTC
- Heure modifiée : 25 août 2022, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDevOpsGuruFullAccess

Description : fournit un accès complet à Amazon DevOps Guru.

AmazonDevOpsGuruFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDevOpsGuruFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2020, 16:38 UTC
- Heure modifiée : 25 août 2022, 18:23 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDevOpsGuruOrganizationsAccess

Description : Fournissez un accès pour activer et gérer Amazon DevOps Guru au sein d'une organisation.

AmazonDevOpsGuruOrganizationsAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDevOpsGuruOrganizationsAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 novembre 2021, 23:50 UTC
- Heure modifiée : 15 novembre 2021, 23:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            ]
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDevOpsGuruReadOnlyAccess

Description : fournit un accès en lecture seule à la console Amazon DevOps Guru.

AmazonDevOpsGuruReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDevOpsGuruReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2020, 16:34 UTC
- Heure modifiée : 25 août 2022, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDevOpsGuruServiceRolePolicy

Description : un rôle lié à un service est requis pour qu'Amazon puisse accéder DevOpsGuru à vos ressources.

AmazonDevOpsGuruServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 01 décembre 2020, 10:24 UTC
- Heure modifiée : 10 janvier 2023, 14:36 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDMSCloudWatchLogsRole

Description : Permet de télécharger les journaux de réplication DMS vers Cloudwatch Logs depuis le compte client.

AmazonDMSCloudWatchLogsRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDMSCloudWatchLogsRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 07 janvier 2016, 23:44 UTC
- Heure modifiée : 23 mai 2023, 21:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDMSRedshiftS3Role

Description : Permet d'accéder à la gestion des paramètres S3 pour les points de terminaison Redshift pour DMS.

AmazonDMSRedshiftS3Role est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonDMSRedshiftS3Role` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 20 avril 2016, 17:05 UTC
- Heure modifiée : 08 juillet 2019, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDMSVPCManagementRole

Description : Permet d'accéder à la gestion des paramètres VPC pour les configurations client AWS gérées

AmazonDMSVPCManagementRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDMSVPCManagementRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 18 novembre 2015, 16:33 UTC
- Heure modifiée : 25 juillet 2024, 15:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDocDB-ElasticServiceRolePolicy

Description : permet DocumentDB-Elastic à Amazon de gérer les AWS ressources en votre nom.

AmazonDocDB-ElasticServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 30 novembre 2022, 14:17 UTC
- Heure modifiée : 30 novembre 2022, 14:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
]
}
}
}
]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDocDBConsoleFullAccess

Description : fournit un accès complet pour gérer Amazon DocumentDB avec la compatibilité avec MongoDB à l'aide du. Console de gestion AWS Notez que cette politique accorde également un accès complet à la publication sur toutes les rubriques SNS du compte, des autorisations pour créer et modifier des instances Amazon EC2 et des configurations VPC, des autorisations pour afficher et répertorier les clés sur Amazon KMS et un accès complet à Amazon RDS et Amazon Neptune.

AmazonDocDBConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDocDBConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 janvier 2019, 20:37 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            }
        }
    }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDocDBElasticFullAccess

Description : fournit un accès complet à Amazon DocumentDB Elastic Clusters et aux autres autorisations requises pour ses dépendances, notamment EC2 SecretsManager, KMS CloudWatch et IAM.

AmazonDocDBElasticFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDocDBElasticFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 juin 2023, 13:51 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDocDBElasticReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon DocDB-Elastic et CloudWatch à ses statistiques.

AmazonDocDBElasticReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDocDBElasticReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 juin 2023, 14:37 UTC
- Heure modifiée : 21 juin 2023, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDocDBFullAccess

Description : fournit un accès complet à Amazon DocumentDB avec compatibilité avec MongoDB.

Notez que cette politique accorde également un accès complet à la publication sur toutes les rubriques SNS du compte et un accès complet à Amazon RDS et Amazon Neptune.

AmazonDocDBFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDocDBFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 janvier 2019, 20:21 UTC
- Heure modifiée : 09 janvier 2019, 20:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:RemoveTagsForResource",
    "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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDocDBReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon DocumentDB avec compatibilité avec MongoDB. Notez que cette politique donne également accès aux ressources Amazon RDS et Amazon Neptune.

AmazonDocDBReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDocDBReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 janvier 2019, 20:30 UTC
- Heure modifiée : 09 janvier 2019, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

Gestion des PC Amazon DRS

Description : Permet d'accéder à la gestion des paramètres VPC pour les configurations clients gérées par Amazon

AmazonDRSVPCManagement est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDRSVPCManagement à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 02 septembre 2015, 00:09 UTC
- Heure modifiée : 02 septembre 2015, 00:09 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDRSVPCManagement

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDynamoDBFullAccess

Description : fournit un accès complet à Amazon DynamoDB via le. Console de gestion AWS

AmazonDynamoDBFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDynamoDBFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 29 janvier 2021, 17:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess`

Version de la politique

Version de la politique : v15 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      ]
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDynamoDBFullAccess_v2

Description : fournit un accès complet à Amazon DynamoDB

AmazonDynamoDBFullAccess_v2 est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDynamoDBFullAccess_v2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 mai 2025, 14:52 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess_v2`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "*"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDynamoDBFullAccesswithDataPipeline

Description : Cette politique est sur la voie de la dépréciation. Consultez la documentation pour obtenir des conseils : <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DynamoDBPipeline.html>. Fournit un accès complet à Amazon DynamoDB, y compris Export/Import en utilisant AWS Data Pipeline via le. Console de gestion AWS

AmazonDynamoDBFullAccesswithDataPipelineest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonDynamoDBFullAccesswithDataPipeline` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 12 novembre 2015, 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonDynamoDBReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon DynamoDB via le. Console de gestion AWS

AmazonDynamoDBReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonDynamoDBReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 18 novembre 2024, 17:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess`

Version de la politique

Version de la politique : v15 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
}
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEBSCSIDriverEKSClusterScopedPolicy

Description : Politique IAM qui permet au compte du service de chauffeur CSI de passer des appels vers des services connexes tels que EC2 en votre nom. Cette politique limite le pilote Amazon EBS CSI à la gestion des volumes EBS et des instantanés uniquement qui appartiennent à un cluster EKS spécifique. Elle nécessite la balise de ressource `ebs.csi.aws.com/cluster-name` pour correspondre à la balise `eks-cluster-name` sur le principal IAM, empêchant ainsi l'accès entre clusters lorsque plusieurs clusters partagent le même. Compte AWS Les opérations d'attachement et de détachement sur les instances sont limitées aux instances marquées soit par la balise `eks:cluster-name` (définie automatiquement par EKS sur les groupes de nœuds gérés) soit par `ebs.csi.aws.com/clusterbalise-name` (pour les instances balisées manuellement).

AmazonEBSCSIDriverEKSClusterScopedPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEBSCSIDriverEKSClusterScopedPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 16 avril 2026, 17:27 UTC
- Heure modifiée : 28 mai 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEBSCSIDriverEKSClusterScopedPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "${aws:PrincipalTag/eks-cluster-name}"
      }
    }
  },
  {
    "Sid" : "CreateVolumesFromAndEnableFSR0nClusterSnapshots",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateVolume",
      "ec2:EnableFastSnapshotRestores"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/ebs.csi.aws.com/cluster-name" : "${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" : "AttachDetachVolumesToEKSSstandardTaggedInstance",
    "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"
      ]
    }
  }
}

```

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEBSCSIDriverPolicy

Description : Politique IAM qui permet au compte du service de chauffeur CSI de passer des appels vers des services connexes tels que EC2 en votre nom.

AmazonEBSCSIDriverPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEBSCSIDriverPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 04 avril 2022, 17:24 UTC
- Heure modifiée : 13 mai 2026, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy`

Version de la politique

Version de la politique : v15 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEBSCSIDriverPolicyV2

Description : Politique IAM qui permet au compte du service de chauffeur EBS CSI de passer des appels en votre nom vers des services connexes tels que EC2. Il limite le pilote Amazon EBS CSI à la gestion des volumes et des instantanés EBS marqués avec la clé `ebs.csi.aws` uniquement. `com/cluster` réglé sur `true`. Les volumes provisionnés par le plug-in de volume Kubernetes intégré à l'arborescence (CSI-migrated volumes) sont également pris en charge via Kubernetes. `io/created-balise de ressource for/pvc /name`.

AmazonEBSCSIDriverPolicyV2 est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEBSCSIDriverPolicyV2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 16 avril 2026, 17:27 UTC
- Heure modifiée : 16 avril 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEBSCSIDriverPolicyV2`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "CreateVolumesFromAndEnableFSR0nManagedSnapshots",
    "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"
      ]
    }
  }
}

```

```
}  
  }  
    }  
  ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEC2ContainerRegistryFullAccess

Description : fournit un accès administratif aux ressources Amazon ECR

AmazonEC2ContainerRegistryFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEC2ContainerRegistryFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 21 décembre 2015, 17:06 UTC
- Heure modifiée : 05 décembre 2020, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
          ]
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEC2ContainerRegistryPowerUser

Description : fournit un accès complet aux référentiels Amazon EC2 Container Registry, mais n'autorise pas la suppression de référentiels ni la modification des règles.

AmazonEC2ContainerRegistryPowerUser est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEC2ContainerRegistryPowerUser à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 21 décembre 2015, 17:05 UTC
- Heure modifiée : 10 décembre 2019, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEC2ContainerRegistryPullOnly

Description : permet d'extraire des images des référentiels Amazon EC2 Container Registry.

AmazonEC2ContainerRegistryPullOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEC2ContainerRegistryPullOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 04 octobre 2024, 16:58 UTC
- Heure modifiée : 04 octobre 2024, 16:58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPullOnly

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchImportUpstreamImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEC2ContainerRegistryReadOnly

Description : fournit un accès en lecture seule aux référentiels Amazon EC2 Container Registry.

AmazonEC2ContainerRegistryReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEC2ContainerRegistryReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 21 décembre 2015, 17:04 UTC
- Heure modifiée : 10 décembre 2019, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEC2ContainerServiceAutoscaleRole

Description : Politique visant à activer la mise à l'échelle automatique des tâches pour Amazon EC2 Container Service

AmazonEC2ContainerServiceAutoscaleRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEC2ContainerServiceAutoscaleRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 12 mai 2016, 23:25 UTC
- Heure modifiée : 05 février 2018, 19:15 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEC2ContainerServiceEventsRole

Description : Politique visant à activer les CloudWatch événements pour EC2 Container Service

AmazonEC2ContainerServiceEventsRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEC2ContainerServiceEventsRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 30 mai 2017, 16:51 UTC
- Heure modifiée : 06 mars 2023, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEC2ContainerServiceforEC2Role

Description : Politique par défaut pour le rôle Amazon EC2 pour Amazon EC2 Container Service.

AmazonEC2ContainerServiceforEC2Role est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEC2ContainerServiceforEC2Role à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 19 mars 2015, 18:45 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*/*"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEC2ContainerServiceRole

Description : Politique par défaut pour le rôle de service Amazon ECS.

AmazonEC2ContainerServiceRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEC2ContainerServiceRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 09 avril 2015, 16:14 UTC
- Heure modifiée : 11 août 2016, 13:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:Describe*",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ]
    }
  ]
}
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEC2FullAccess

Description : Fournit un accès complet à Amazon EC2 via le Console de gestion AWS.

AmazonEC2FullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEC2FullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 27 novembre 2018, 02:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2FullAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
          ]
        }
      }
    }
  ]
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEC2ImageReferencesAccessPolicy

Description : fournit un accès en lecture seule pour analyser tous les types de ressources pris en charge à la recherche de données pertinentes lors de leur utilisation. DescribeImageReferences

AmazonEC2ImageReferencesAccessPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEC2ImageReferencesAccessPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 août 2025, 19:19 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ImageReferencesAccessPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
          ]
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEC2ReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon EC2 via le Console de gestion AWS.

AmazonEC2ReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEC2ReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 12 février 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEC2RoleforAWSCodeDeploy

Description : fournit à EC2 un accès au compartiment S3 pour télécharger la révision. Ce rôle est requis par l' CodeDeploy agent sur les instances EC2.

AmazonEC2RoleforAWSCodeDeploy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEC2RoleforAWSCodeDeploy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 19 mai 2015, 18:10 UTC
- Heure modifiée : 20 mars 2017, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEC2RoleforAWSCodeDeployLimited

Description : fournit à EC2 un accès limité au compartiment S3 pour télécharger la révision. Ce rôle est requis par l' CodeDeploy agent sur les instances EC2.

AmazonEC2RoleforAWSCodeDeployLimited est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEC2RoleforAWSCodeDeployLimited à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 24 août 2020, 17:55 UTC
- Heure modifiée : 20 janvier 2022, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEC2RoleforDataPipelineRole

Description : Politique par défaut pour le rôle de service Amazon EC2 Role for Data Pipeline.

AmazonEC2RoleforDataPipelineRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEC2RoleforDataPipelineRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 22 février 2016, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [  
        "*"   
    ]  
  }  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

Rôle Amazon EC2 pour SSM

Description : Cette politique sera bientôt obsolète. Utilisez AmazonSSMManagedInstanceCore la politique pour activer les fonctionnalités principales du service AWS Systems Manager sur les instances EC2. Pour plus d'informations, consultez <https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-instance-profile.html>.

AmazonEC2RoleforSSMest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEC2RoleforSSM à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 29 mai 2015, 17:48 UTC
- Heure modifiée : 24 janvier 2019, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEC2RolePolicyForLaunchWizard

Description : Politique gérée pour le rôle de LaunchWizard service Amazon pour EC2

AmazonEC2RolePolicyForLaunchWizard est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEC2RolePolicyForLaunchWizard à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 novembre 2019, 08:05 UTC
- Heure modifiée : 18 août 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEC2SpotFleetAutoscaleRole

Description : Politique visant à activer la mise à l'échelle automatique pour Amazon EC2 Spot Fleet

AmazonEC2SpotFleetAutoscaleRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEC2SpotFleetAutoscaleRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 19 août 2016, 18:27 UTC
- Heure modifiée : 18 février 2019, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEC2SpotFleetTaggingRole

Description : permet à EC2 Spot Fleet de demander, de résilier et de baliser des instances Spot en votre nom.

AmazonEC2SpotFleetTaggingRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonEC2SpotFleetTaggingRole` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 29 juin 2017, 18:19 UTC
- Heure modifiée : 23 avril 2020, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*:*:*/*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

Amazon ECS_FullAccess

Description : fournit un accès administratif aux ressources Amazon ECS et active les fonctionnalités ECS en accédant à d'autres ressources de AWS service, notamment des VPC, des groupes Auto Scaling et des CloudFormation piles.

AmazonECS_FullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonECS_FullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 novembre 2017, 21:36 UTC
- Heure modifiée : 02 septembre 2026, 14:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECS_FullAccess`

Version de la politique

Version de la politique : v22 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            ]
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonECSComputeServiceRolePolicy

Description : Politique permettant à Amazon ECS Compute de gérer vos instances EC2 et les ressources associées dans le cadre des instances gérées par ECS

AmazonECSComputeServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 24 mars 2025, 17:37 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSComputeServiceRolePolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonECSInfrastructureRoleforExpressGatewayServices

Description : Ces autorisations permettent à Amazon ECS de provisionner et de gérer automatiquement les composants d'infrastructure requis pour les services Express Gateway, notamment l'équilibrage de charge, les groupes de sécurité, les certificats SSL et les configurations de dimensionnement automatique.

AmazonECSInfrastructureRoleforExpressGatewayServices est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonECSInfrastructureRoleforExpressGatewayServices à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 12 novembre 2025, 20:34 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRoleforExpressGatewayServices`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/AmazonECSTaskManaged" : "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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonECSInfrastructureRoleForGatewayHostSharedALB

Description : Politique par défaut pour le rôle d'infrastructure Amazon ECS pour Amazon ECS Service Gateway Services.

AmazonECSInfrastructureRoleForGatewayHostSharedALB est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonECSInfrastructureRoleForGatewayHostSharedALB à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 25 septembre 2026, 21:17 UTC
- Heure modifiée : 25 septembre 2026, 21:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRoleForGatewayHostSharedALB`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonECSInfrastructureRolePolicyForLoadBalancers

Description : donne accès à d'autres ressources de AWS service nécessaires pour gérer les équilibreurs de charge associés aux charges de travail ECS en votre nom.

AmazonECSInfrastructureRolePolicyForLoadBalancersest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonECSInfrastructureRolePolicyForLoadBalancers` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 juillet 2025, 16:37 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForLoadBalancers`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*/*/*/*"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonECSInfrastructureRolePolicyForManagedInstances

Description : fournit un accès à ECS pour créer et gérer des ressources gérées EC2

AmazonECSInfrastructureRolePolicyForManagedInstances est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonECSInfrastructureRolePolicyForManagedInstances à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 septembre 2025, 18:04 UTC
- Heure modifiée : 15 septembre 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForManagedInstances`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity

Description : fournit un accès administratif à l'autorité de certification privée, à AWS Secrets Manager et à d'autres Services AWS outils nécessaires pour gérer les fonctionnalités TLS d'ECS Service Connect en votre nom.

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 19 janvier 2024, 20:08 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/AmazonECManaged" : "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/AmazonECManaged" : "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"
            }
        }
    }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonECSInfrastructureRolePolicyForVolumes

Description : donne accès à d'autres ressources AWS de service nécessaires pour gérer les volumes associés aux charges de travail ECS en votre nom.

AmazonECSInfrastructureRolePolicyForVolumes est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonECSInfrastructureRolePolicyForVolumes à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 10 janvier 2024, 22:56 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/AmazonECSManaged" : "arn:aws:ecs:*:*:task/*"
    },
    "StringEquals" : {
      "aws:ResourceTag/AmazonECSManaged" : "true"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonECSInfrastructureRolePolicyForVpcLattice

Description : Permet d'accéder aux autres ressources de AWS service nécessaires pour gérer la fonctionnalité VPC Lattice dans les charges de travail ECS en votre nom.

AmazonECSInfrastructureRolePolicyForVpcLattice est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonECSInfrastructureRolePolicyForVpcLattice à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 novembre 2024, 20:02 UTC
- Heure modifiée : 29 septembre 2026, 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForVpcLattice`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "*"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonECSInstanceRolePolicyForManagedInstances

Description : Politique par défaut pour le rôle d'instance Amazon ECS pour les instances gérées Amazon ECS.

AmazonECSInstanceRolePolicyForManagedInstances est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonECSInstanceRolePolicyForManagedInstances à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 septembre 2025, 23:49 UTC
- Heure modifiée : 02 juillet 2026, 02:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInstanceRolePolicyForManagedInstances`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonECSServiceRolePolicy

Description : Politique permettant à Amazon ECS de gérer votre cluster.

AmazonECSServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 14 octobre 2017, 01:18 UTC
- Heure modifiée : 22 avril 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy`

Version de la politique

Version de la politique : v24 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonECSTaskExecutionRolePolicy

Description : Permet d'accéder à d'autres ressources de AWS service nécessaires à l'exécution des tâches Amazon ECS

AmazonECSTaskExecutionRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonECSTaskExecutionRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 16 novembre 2017, 18:48 UTC
- Heure modifiée : 16 novembre 2017, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEFSCSIDriverPolicy

Description : fournit un accès de gestion aux ressources EFS et un accès en lecture à EC2

AmazonEFSCSIDriverPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEFSCSIDriverPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 25 juillet 2023, 20:10 UTC
- Heure modifiée : 25 juillet 2023, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEKS_CNI_Policy

Description : Cette politique fournit au plug-in Amazon VPC CNI (amazon-vpc-cni-k8s) les autorisations dont il a besoin pour modifier la configuration de l'adresse IP sur vos nœuds de travail EKS. Cet ensemble d'autorisations permet au CNI de répertorier, de décrire et de modifier les interfaces réseau Elastic en votre nom. Plus d'informations sur le plug-in AWS VPC CNI sont disponibles ici : <https://github.com/aws/amazon-vpc-cni-k8s>

AmazonEKS_CNI_Policy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEKS_CNI_Policy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 mai 2018, 21:07 UTC
- Heure modifiée : 04 mars 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEKSBLOCKStoragePolicy

Description : Politique associée au rôle de cluster EKS qui accorde des autorisations pour gérer les ressources de stockage par blocs du cluster.

AmazonEKSBLOCKStoragePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEKSBLOCKStoragePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 octobre 2024, 20:18 UTC
- Heure modifiée : 30 octobre 2024, 20:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSBLOCKStoragePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      ]
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEKSBLOCKStoragePolicyV2

Description : Politique associée au rôle de cluster EKS qui accorde des autorisations pour gérer les ressources de stockage par blocs du cluster.

AmazonEKSBLOCKStoragePolicyV2 est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEKSBLOCKStoragePolicyV2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 mai 2026, 16:27 UTC
- Heure modifiée : 11 mai 2026, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSBLOCKStoragePolicyV2`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ]
}
}
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEKSClusterPolicy

Description : Cette politique fournit à Kubernetes les autorisations dont il a besoin pour gérer les ressources en votre nom. Kubernetes a besoin d' `Ec2:CreateTags` autorisations pour placer des informations d'identification sur les ressources EC2, y compris, mais sans s'y limiter, les instances, les groupes de sécurité et les interfaces réseau Elastic.

AmazonEKSClusterPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEKSClusterPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 mai 2018, 21:06 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSClusterPolicy`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEKSClusterPolicy

Description : Politique associée au rôle de cluster EKS qui accorde des autorisations pour gérer les ressources de calcul du cluster.

AmazonEKSClusterPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEKSClusterPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 01 novembre 2024, 21:46 UTC
- Heure modifiée : 18 mai 2026, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSCoordinatePolicy`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEKSCredentialsServiceRolePolicy

Description : Cette politique permet à Amazon EKS de gérer les AWS ressources du connecteur EKS

AmazonEKSCredentialsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 04 septembre 2021, 20:31 UTC
- Heure modifiée : 15 octobre 2025, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSCredentialsServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEKSDashboardConsoleReadOnly

Description : fournit un accès en lecture seule pour afficher le tableau de bord dans la console Amazon EKS. Le tableau de bord regroupe des informations sur plusieurs clusters et les ressources associées à l'aide des AWS organisations.

AmazonEKSDashboardConsoleReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEKSDashboardConsoleReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 juin 2025, 17:22 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSDashboardConsoleReadOnly`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEKSDashboardServiceRolePolicy

Description : Cette politique permet au tableau de bord Amazon EKS d'accéder aux informations relatives à l'ensemble de l'organisation et de les afficher. La politique permet au service EKS Dashboard de recueillir des informations sur la structure et les comptes de votre AWS organisation.

AmazonEKSDashboardServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 08 mai 2025, 19:07 UTC
- Heure modifiée : 08 mai 2025, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSDashboardServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEKSFargatePodExecutionRolePolicy

Description : Permet d'accéder à d'autres ressources de AWS service nécessaires pour exécuter les modules Amazon EKS sur AWS Fargate

AmazonEKSFargatePodExecutionRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEKSFargatePodExecutionRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 novembre 2019, 04:34 UTC

- Heure modifiée : 22 novembre 2019, 04:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEKSFargateServiceRolePolicy

Description : Cette politique accorde les autorisations nécessaires à Amazon EKS pour exécuter des tâches Fargate.

AmazonEKSFargateServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 22 novembre 2019, 04:36 UTC
- Heure modifiée : 22 novembre 2019, 04:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSFargateServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEKSLoadBalancingPolicy

Description : Politique associée au rôle de cluster EKS qui accorde des autorisations pour gérer les ressources d'équilibrage de charge du cluster.

AmazonEKSLoadBalancingPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEKSLoadBalancingPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 octobre 2024, 20:18 UTC
- Heure modifiée : 20 août 2026, 23:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSLoadBalancingPolicy

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEKSLocalOutpostClusterPolicy

Description : Cette politique fournit des autorisations aux instances du plan de contrôle du cluster local EKS exécutées sur votre compte afin de gérer les ressources en votre nom.

AmazonEKSLocalOutpostClusterPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEKSLocalOutpostClusterPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 août 2022, 21:56 UTC
- Heure modifiée : 24 octobre 2024, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*:*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEKSLocalOutpostServiceRolePolicy

Description : permet à Amazon EKS Local d'appeler AWS les services en votre nom.

AmazonEKSLocalOutpostServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 23 août 2022, 21:53 UTC
- Heure modifiée : 26 juin 2025, 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSLocalOutpostServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"   
  }  
]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEKSMCPReadOnlyAccess

Description : fournit un accès en lecture seule au service Amazon EKS MCP. Cette politique autorise l'utilisation d'outils en lecture seule dans le service EKS MCP destinés à l'observabilité, au dépannage, à la récupération d'informations sur les ressources EKS et à l'obtention de suggestions. EKS-optimized

AmazonEKSMCPReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEKSMCPReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 novembre 2025, 17:19 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSMCPReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEKSNetworkingPolicy

Description : Politique associée au rôle de cluster EKS qui accorde des autorisations pour gérer les ressources réseau du cluster.

AmazonEKSNetworkingPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEKSNetworkingPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 octobre 2024, 22:34 UTC
- Heure modifiée : 21 août 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSNetworkingPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
      }
    }
  ]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEKSServicePolicy

Description : Cette politique permet à Amazon Elastic Container Service pour Kubernetes de créer et de gérer les ressources nécessaires au fonctionnement des clusters EKS.

AmazonEKSServicePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEKSServicePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 mai 2018, 21:08 UTC
- Heure modifiée : 14 octobre 2024, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSServicePolicy`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEKSServiceRolePolicy

Description : Service-Linked rôle requis pour qu'Amazon EKS puisse appeler AWS les services en votre nom.

AmazonEKSServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 21 février 2020, 20:10 UTC
- Heure modifiée : 01 octobre 2026, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy`

Version de la politique

Version de la politique : v28 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
      }
    }
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEKSVPCResourceController

Description : Politique utilisée par le contrôleur de ressources VPC pour gérer l'ENI et les adresses IP des nœuds de travail.

AmazonEKSVPCResourceController est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEKSVPCResourceController à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 août 2020, 00:55 UTC
- Heure modifiée : 12 août 2020, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSVPCResourceController`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEKSWorkerNodeMinimalPolicy

Description : Cette politique permet aux nœuds de travail Amazon EKS de se connecter aux clusters Amazon EKS.

AmazonEKSWorkerNodeMinimalPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEKSWorkerNodeMinimalPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 octobre 2024, 20:03 UTC

- Heure modifiée : 02 octobre 2024, 20:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSTaskRoleMinimalPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkerNodePermissions",
      "Effect" : "Allow",
      "Action" : [
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEKSTaskRolePolicy

Description : Cette politique permet aux nœuds de travail Amazon EKS de se connecter aux clusters Amazon EKS.

`AmazonEKSElasticContainerWorkerNodePolicy` est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonEKSTaskRolePolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 mai 2018, 21:09 UTC
- Heure modifiée : 27 novembre 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSEWorkerNodePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"    
  }  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElastiCacheFullAccess

Description : fournit un accès complet à Amazon ElastiCache via le Console de gestion AWS.

AmazonElastiCacheFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonElastiCacheFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 28 novembre 2023, 03:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElastiCacheReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon ElastiCache via le Console de gestion AWS.

AmazonElastiCacheReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonElastiCacheReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 06 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElasticContainerRegistryPublicFullAccess

Description : Fournit un accès administratif aux ressources publiques d'Amazon ECR

AmazonElasticContainerRegistryPublicFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonElasticContainerRegistryPublicFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2020, 17:25 UTC
- Heure modifiée : 01 décembre 2020, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElasticContainerRegistryPublicPowerUser

Description : fournit un accès complet aux référentiels publics Amazon ECR, mais n'autorise pas la suppression de référentiels ni la modification des règles.

AmazonElasticContainerRegistryPublicPowerUser est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonElasticContainerRegistryPublicPowerUser à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2020, 16:16 UTC
- Heure modifiée : 01 décembre 2020, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicPowerUser`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElasticContainerRegistryPublicReadOnly

Description : fournit un accès en lecture seule aux référentiels publics Amazon ECR.

AmazonElasticContainerRegistryPublicReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonElasticContainerRegistryPublicReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 01 décembre 2020, 17:27 UTC
- Heure modifiée : 01 décembre 2020, 17:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElasticFileSystemClientFullAccess

Description : fournit un accès client root à un système de fichiers Amazon EFS

AmazonElasticFileSystemClientFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonElasticFileSystemClientFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 janvier 2020, 16:27 UTC
- Heure modifiée : 13 janvier 2020, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElasticFileSystemClientReadOnlyAccess

Description : fournit un accès client en lecture seule à un système de fichiers Amazon EFS

AmazonElasticFileSystemClientReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonElasticFileSystemClientReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 janvier 2020, 16:24 UTC
- Heure modifiée : 13 janvier 2020, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElasticFileSystemClientReadWriteAccess

Description : fournit un accès client en lecture et en écriture à un système de fichiers Amazon EFS

AmazonElasticFileSystemClientReadWriteAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonElasticFileSystemClientReadWriteAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 janvier 2020, 16:21 UTC
- Heure modifiée : 13 janvier 2020, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElasticFileSystemFullAccess

Description : fournit un accès complet à Amazon EFS via le Console de gestion AWS.

AmazonElasticFileSystemFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonElasticFileSystemFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 mai 2015, 16:22 UTC
- Heure modifiée : 07 novembre 2024, 19:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElasticFileSystemReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon EFS via le Console de gestion AWS.

AmazonElasticFileSystemReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonElasticFileSystemReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 mai 2015, 16:25 UTC
- Heure modifiée : 07 novembre 2024, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElasticFileSystemServiceRolePolicy

Description : Permet à Amazon Elastic File System de gérer les AWS ressources en votre nom

AmazonElasticFileSystemServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle

- Heure de création : 05 novembre 2019, 16:52 UTC
- Heure modifiée : 07 novembre 2024, 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElasticFileSystemsUtils

Description : permet aux clients d'utiliser AWS Systems Manager pour gérer automatiquement le package des utilitaires Amazon EFS (amazon-efs-utils) sur leurs instances EC2 et de les utiliser CloudWatchLog pour recevoir des notifications de montage du système de fichiers EFS. success/failure

AmazonElasticFileSystemsUtilsest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonElasticFileSystemsUtils à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 septembre 2020, 15:16 UTC

- Heure modifiée : 07 avril 2026, 13:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ]
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElasticMapReduceEditorsRole

Description : Politique par défaut pour le rôle de service Amazon Elastic MapReduce Editors.

AmazonElasticMapReduceEditorsRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonElasticMapReduceEditorsRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 16 novembre 2018, 21:55 UTC
- Heure modifiée : 09 février 2023, 22:39 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceEditorsRole`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ]
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElasticMapReduceforAutoScalingRole

Description : Amazon Elastic MapReduce pour Auto Scaling. Rôle permettant à Auto Scaling d'ajouter et de supprimer des instances de votre cluster EMR.

AmazonElasticMapReduceforAutoScalingRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonElasticMapReduceforAutoScalingRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 18 novembre 2016, 01:09 UTC
- Heure modifiée : 18 novembre 2016, 01:09 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElasticMapReduceforEC2Role

Description : Politique par défaut pour le rôle de service Amazon Elastic MapReduce for EC2.

AmazonElasticMapReduceforEC2Role est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonElasticMapReduceforEC2Role à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 11 août 2017, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
]
}
]
}
```


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElasticMapReduceFullAccess

Description : Cette politique est sur la voie de la dépréciation. Consultez la documentation pour obtenir des conseils : <https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html>. Fournit un accès complet à Amazon Elastic MapReduce et aux services sous-jacents dont il a besoin, tels que EC2 et S3

AmazonElasticMapReduceFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonElasticMapReduceFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 11 septembre 2026, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            ]
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElasticMapReducePlacementGroupPolicy

Description : Politique permettant à EMR de créer, de décrire et de supprimer des groupes de placement EC2.

AmazonElasticMapReducePlacementGroupPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonElasticMapReducePlacementGroupPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 septembre 2020, 00:37 UTC
- Heure modifiée : 29 septembre 2020, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElasticMapReduceReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon Elastic MapReduce via le Console de gestion AWS.

AmazonElasticMapReduceReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonElasticMapReduceReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC

- Heure modifiée : 29 juillet 2020, 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElasticMapReduceRole

Description : Cette politique est sur la voie de la dépréciation. Consultez la documentation pour obtenir des conseils : Politique <https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html>. par défaut pour le rôle de MapReduce service Amazon Elastic.

AmazonElasticMapReduceRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonElasticMapReduceRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 24 juin 2020, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElasticsearchServiceRolePolicy

Description : Autorisez Amazon Elasticsearch Service à accéder à d'autres AWS services tels que les API réseau EC2 en votre nom.

AmazonElasticsearchServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 07 juillet 2017, 00:15 UTC
- Heure modifiée : 22 juin 2026, 12:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticsearchServiceRolePolicy`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElasticTranscoder_FullAccess

Description : accorde aux utilisateurs un accès complet à Elastic Transcoder et l'accès aux services associés nécessaires pour bénéficier de toutes les fonctionnalités d'Elastic Transcoder.

AmazonElasticTranscoder_FullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonElasticTranscoder_FullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 avril 2018, 18:59 UTC
- Heure modifiée : 10 juin 2019, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElasticTranscoder_JobsSubmitter

Description : autorise les utilisateurs à modifier les préférences, à soumettre des tâches et à consulter les paramètres d'Elastic Transcoder. Cette politique accorde également un accès en lecture seule à certains autres services nécessaires à l'utilisation de la console Elastic Transcode, notamment S3, IAM et SNS.

AmazonElasticTranscoder_JobsSubmitter est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonElasticTranscoder_JobsSubmitter à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 juin 2018, 21:12 UTC
- Heure modifiée : 10 juin 2019, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElasticTranscoder_ReadOnlyAccess

Description : accorde aux utilisateurs un accès en lecture seule à Elastic Transcoder et un accès à la liste des services associés.

AmazonElasticTranscoder_ReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonElasticTranscoder_ReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 juin 2018, 21:09 UTC
- Heure modifiée : 10 juin 2019, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
"Statement" : [
  {
    "Action" : [
      "elastictranscoder:Read*",
      "elastictranscoder:List*",
      "s3:ListAllMyBuckets",
      "s3:ListBucket",
      "iam:ListRoles",
      "sns:ListTopics"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonElasticTranscoderRole

Description : Politique par défaut pour le rôle de service Amazon Elastic Transcoder.

AmazonElasticTranscoderRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonElasticTranscoderRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 13 juin 2019, 22:48 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEMRCleanupPolicy

Description : autorise les actions requises par EMR pour mettre fin et supprimer des ressources AWS EC2 si le rôle de service EMR a perdu cette capacité.

AmazonEMRCleanupPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 26 septembre 2017, 23:54 UTC
- Heure modifiée : 29 septembre 2020, 21:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ]
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEMRContainersServiceRolePolicy

Description : Permet d'accéder aux autres ressources AWS de service nécessaires à l'exécution d'Amazon EMR

AmazonEMRContainersServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 09 décembre 2020, 00:38 UTC
- Heure modifiée : 24 juillet 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      ]
    }
  }
}
}

```



```
]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEMRFullAccessPolicy_v2

Description : fournit un accès complet à Amazon EMR

AmazonEMRFullAccessPolicy_v2 est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEMRFullAccessPolicy_v2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 mars 2021, 01:50 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEMRReadOnlyAccessPolicy_v2

Description : fournit un accès en lecture seule à Amazon EMR et aux CloudWatch métriques associées.

AmazonEMRReadOnlyAccessPolicy_v2 est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEMRReadOnlyAccessPolicy_v2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 mars 2021, 01:39 UTC
- Heure modifiée : 02 août 2023, 19:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEMRServerlessServiceRolePolicy

Description : Permet d'accéder aux autres ressources AWS de service nécessaires à l'exécution d'Amazon EMRServerless

AmazonEMRServerlessServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 20 mai 2022, 23:15 UTC
- Heure modifiée : 25 janvier 2024, 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
          ]
        }
      }
    }
  ]
}
```



```
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEMRServicePolicy_v2

Description : Cette politique est utilisée pour le rôle de service Amazon EMR et ne doit PAS être utilisée pour les autres utilisateurs ou rôles IAM de votre compte. La politique accorde des autorisations pour créer et gérer des ressources associées à l'EMR et aux services connexes nécessaires au fonctionnement de votre cluster EMR.

AmazonEMRServicePolicy_v2 est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEMRServicePolicy_v2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 12 mars 2021, 01:11 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEMRServicePolicyForSessions

Description : fournit les autorisations nécessaires pour provisionner et gérer les équilibreurs de charge réseau, les services de point de terminaison VPC et les groupes de sécurité requis pour les sessions interactives Amazon EMR Spark Connect sur EMR sur les clusters EC2.

AmazonEMRServicePolicyForSession est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonEMRServicePolicyForSessions` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 22 juin 2026, 19:57 UTC
- Heure modifiée : 22 juin 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicyForSessions`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonESCognitoAccess

Description : fournit un accès limité au service de configuration Amazon Cognito.

AmazonESCognitoAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonESCognitoAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 février 2018, 22:29 UTC
- Heure modifiée : 20 décembre 2021, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESCognitoAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
          ]
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonESFullAccess

Description : fournit un accès complet au service de configuration Amazon ES.

AmazonESFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonESFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 octobre 2015, 19:14 UTC
- Heure modifiée : 01 octobre 2015, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonESReadOnlyAccess

Description : fournit un accès en lecture seule au service de configuration Amazon ES.

AmazonESReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonESReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 octobre 2015, 19:18 UTC
- Heure modifiée : 3 octobre 2018, 03:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEventBridgeApiDestinationsServiceRolePolicy

Description : Permet d'accéder EventBridge aux ressources de Secret Manager en votre nom.

AmazonEventBridgeApiDestinationsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle

- Heure de création : 11 février 2021, 20:52 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeApiDestinationsServiceRolePolicy`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  }
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEventBridgeFullAccess

Description : fournit un accès complet à Amazon EventBridge.

AmazonEventBridgeFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEventBridgeFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 juillet 2019, 14:08 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEventBridgePipesFullAccess

Description : fournit un accès complet à Amazon EventBridge Pipes.

AmazonEventBridgePipesFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEventBridgePipesFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2022, 17:03 UTC
- Heure modifiée : 01 décembre 2022, 17:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEventBridgePipesOperatorAccess

Description : fournit un accès en lecture seule et aux opérateurs (possibilité d'arrêter et de démarrer l'exécution de Pipes) à Amazon EventBridge Pipes.

AmazonEventBridgePipesOperatorAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEventBridgePipesOperatorAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2022, 17:04 UTC
- Heure modifiée : 01 décembre 2022, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "pipes:StartPipe",
        "pipes:StopPipe"
      ]
    }
  ]
}
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEventBridgePipesReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon EventBridge Pipes.

AmazonEventBridgePipesReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEventBridgePipesReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2022, 17:04 UTC
- Heure modifiée : 01 décembre 2022, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEventBridgeReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon EventBridge.

AmazonEventBridgeReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEventBridgeReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 juillet 2019, 13:59 UTC

- Heure modifiée : 24 septembre 2026, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEventBridgeSchedulerFullAccess

Description : La politique AmazonEventBridgeSchedulerFullAccess gérée autorise l'utilisation de toutes les actions du EventBridge planificateur pour les planifications et les groupes de planifications.

AmazonEventBridgeSchedulerFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEventBridgeSchedulerFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 10 novembre 2022, 18:37 UTC
- Heure modifiée : 12 février 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

```
}  
  }  
    }  
  ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEventBridgeSchedulerReadOnlyAccess

Description : La politique AmazonEventBridgeSchedulerReadOnlyAccess gérée accorde des autorisations en lecture seule pour afficher les détails de vos plannings et de vos groupes de plannings

AmazonEventBridgeSchedulerReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEventBridgeSchedulerReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 10 novembre 2022, 18:50 UTC
- Heure modifiée : 02 avril 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEventBridgeSchemasFullAccess

Description : fournit un accès complet à Amazon EventBridge Schemas.

AmazonEventBridgeSchemasFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEventBridgeSchemasFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2019, 23:12 UTC
- Heure modifiée : 28 novembre 2019, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEventBridgeSchemasReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon EventBridge Schemas.

AmazonEventBridgeSchemasReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonEventBridgeSchemasReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2019, 23:05 UTC
- Heure modifiée : 01 mai 2020, 00:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEventBridgeSchemasServiceRolePolicy

Description : accorde des autorisations aux règles gérées créées par les EventBridge schémas Amazon.

AmazonEventBridgeSchemasServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 27 novembre 2019, 01:10 UTC
- Heure modifiée : 27 novembre 2019, 01:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
]
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonEVSServiceRolePolicy

Description : Autorise EVS à gérer les ressources en votre nom

AmazonEVSServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 16 mai 2025, 23:37 UTC
- Heure modifiée : 22 mars 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEVSServiceRolePolicy`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonFISServiceRolePolicy

Description : Politique permettant à la AWS FIS de gérer la surveillance et la sélection des ressources pour les expériences.

AmazonFISServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 21 décembre 2020, 21:18 UTC
- Heure modifiée : 25 octobre 2022, 09:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonForecastFullAccess

Description : donne accès à toutes les actions pour Amazon Forecast

AmazonForecastFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonForecastFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 janvier 2019, 01:52 UTC
- Heure modifiée : 18 janvier 2019, 01:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonForecastFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
"Effect" : "Allow",
"Action" : [
  "iam:PassRole"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "iam:PassedToService" : "forecast.amazonaws.com"
  }
}
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonFraudDetectorFullAccessPolicy

Description : donne accès à toutes les actions d'Amazon Fraud Detector

AmazonFraudDetectorFullAccessPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonFraudDetectorFullAccessPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 décembre 2019, 22:46 UTC
- Heure modifiée : 03 décembre 2019, 22:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonFreeRTOSFullAccess

Description : Politique d'accès complet pour Amazon FreeRTOS

AmazonFreeRTOSFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonFreeRTOSFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2017, 15:32 UTC
- Heure modifiée : 29 novembre 2017, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFreeRTOSFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonFreeRTOSOTAUpdate

Description : Permet à l'utilisateur d'accéder à la mise à jour OTA d'Amazon FreeRTOS

AmazonFreeRTOSOTAUpdate est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonFreeRTOSOTAUpdate à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 27 août 2018, 22:43 UTC
- Heure modifiée : 18 décembre 2020, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonFSxConsoleFullAccess

Description : Fournit un accès complet à Amazon FSx et un accès aux AWS services associés via le Console de gestion AWS.

AmazonFSxConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonFSxConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2018, 16:36 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess`

Version de la politique

Version de la politique : v20 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
}

```

```
}  
  }  
] }  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonFSxConsoleReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon FSx et un accès aux AWS services associés via le Console de gestion AWS.

AmazonFSxConsoleReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonFSxConsoleReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2018, 16:35 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonFSxFullAccess

Description : fournit un accès complet à Amazon FSx et aux AWS services associés.

AmazonFSxFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonFSxFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2018, 16:34 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxFullAccess`

Version de la politique

Version de la politique : v13 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonFSxReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon FSx.

AmazonFSxReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonFSxReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2018, 16:33 UTC
- Heure modifiée : 28 novembre 2018, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonFSxServiceRolePolicy

Description : Permet à Amazon FSx de gérer les AWS ressources en votre nom

AmazonFSxServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 28 novembre 2018, 10:38 UTC
- Heure modifiée : 22 juillet 2025, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonGlacierFullAccess

Description : fournit un accès complet à Amazon Glacier via le Console de gestion AWS.

AmazonGlacierFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonGlacierFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 06 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonGlacierReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon Glacier via le Console de gestion AWS.

AmazonGlacierReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonGlacierReadOnlyAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 05 mai 2016, 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonGrafanaAthenaAccess

Description : Cette politique donne accès à Amazon Athena et aux dépendances nécessaires pour permettre d'interroger et d'écrire des résultats dans s3 à partir du plug-in Amazon Athena dans Amazon Grafana.

AmazonGrafanaAthenaAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonGrafanaAthenaAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 22 novembre 2021, 17:11 UTC
- Heure modifiée : 22 novembre 2021, 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonGrafanaCloudWatchAccess

Description : Cette politique donne accès à Amazon CloudWatch et aux dépendances nécessaires pour l'utiliser CloudWatch comme source de données dans Amazon Managed Grafana.

AmazonGrafanaCloudWatchAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonGrafanaCloudWatchAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 24 mars 2023, 22:41 UTC
- Heure modifiée : 24 mars 2023, 22:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonGrafanaRedshiftAccess

Description : Cette politique accorde un accès limité à Amazon Redshift et aux dépendances nécessaires pour utiliser le plug-in Amazon Redshift dans Amazon Grafana.

AmazonGrafanaRedshiftAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonGrafanaRedshiftAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 26 novembre 2021, 23:15 UTC
- Heure modifiée : 26 novembre 2021, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]

```

```
}  
  }  
  ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonGrafanaServiceLinkedRolePolicy

Description : Permet d'accéder aux AWS ressources gérées ou utilisées par Amazon Grafana.

AmazonGrafanaServiceLinkedRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 08 novembre 2022, 23:10 UTC
- Heure modifiée : 08 novembre 2022, 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonGuardDutyFullAccess

Description : fournit un accès complet pour utiliser Amazon GuardDuty.

AmazonGuardDutyFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonGuardDutyFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2017, 22:31 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            ]
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonGuardDutyFullAccess_v2

Description : fournit un accès complet pour utiliser Amazon GuardDuty

AmazonGuardDutyFullAccess_v2 est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonGuardDutyFullAccess_v2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 juin 2025, 20:22 UTC
- Heure modifiée : 28 septembre 2026, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess_v2`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonGuardDutyMalwareProtectionServiceRolePolicy

Description : la protection contre les GuardDuty programmes malveillants utilise le rôle lié aux services (SLR) nommé. AWSServiceRoleForAmazonGuardDutyMalwareProtection Ce rôle lié à un service permet à la protection contre les GuardDuty programmes malveillants d'effectuer des analyses sans agent pour détecter les programmes malveillants. Il permet GuardDuty de créer des instantanés dans votre compte et de partager les instantanés avec le compte de GuardDuty service pour détecter les logiciels malveillants. Il évalue ces instantanés partagés et inclut les métadonnées de l'instance EC2 récupérées dans les résultats de la protection GuardDuty contre les programmes

malveillants. Le rôle `AWSServiceRoleForAmazonGuardDutyMalwareProtection` lié à un service fait confiance au service `malware-protection.guardduty.amazonaws.com` pour assumer le rôle.

`AmazonGuardDutyMalwareProtectionServiceRolePolicy` est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 19 juillet 2022, 19:06 UTC
- Heure modifiée : 25 janvier 2024, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/guarddduty/*"
  },
  {
    "Sid" : "GuardDutyLogStreamPermission",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:PutLogEvents",
      "logs:DescribeLogStreams"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/guarddduty/*: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"
      }
    }
  }
]

```

```
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonGuardDutyReadOnlyAccess

Description : fournit un accès en lecture seule aux GuardDuty ressources Amazon

AmazonGuardDutyReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonGuardDutyReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2017, 22:29 UTC
- Heure modifiée : 16 novembre 2023, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonGuardDutyServiceRolePolicy

Description : Autoriser l'accès aux AWS ressources utilisées ou gérées par Amazon Guard Duty

AmazonGuardDutyServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 28 novembre 2017, 20:12 UTC
- Heure modifiée : 09 septembre 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy`

Version de la politique

Version de la politique : v13 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/guarddduty/*",
    "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" : "*"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonHealthLakeFullAccess

Description : fournit un accès complet au HealthLake service Amazon.

AmazonHealthLakeFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonHealthLakeFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 février 2021, 01:07 UTC
- Heure modifiée : 17 février 2021, 01:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonHealthLakeReadOnlyAccess

Description : fournit un accès en lecture seule au HealthLake service Amazon.

AmazonHealthLakeReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonHealthLakeReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 février 2021, 02:43 UTC
- Heure modifiée : 4 août 2026, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonHoneycodeFullAccess

Description : fournit un accès complet à Honeycode via le SDK Console de gestion AWS et le SDK.

AmazonHoneycodeFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonHoneycodeFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 juin 2020, 20:28 UTC
- Heure modifiée : 24 juin 2020, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonHoneycodeReadOnlyAccess

Description : fournit un accès en lecture seule à Honeycode via le SDK Console de gestion AWS et le SDK.

AmazonHoneycodeReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonHoneycodeReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 juin 2020, 20:28 UTC
- Heure modifiée : 01 décembre 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonHoneycodeServiceRolePolicy

Description : un rôle lié à un service est requis pour qu'Amazon Honeycode puisse accéder à vos ressources.

AmazonHoneycodeServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 18 novembre 2020, 18:03 UTC
- Heure modifiée : 18 novembre 2020, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sso:GetManagedApplicationInstance"
      ]
    }
  ]
}
```

```
    ],  
    "Resource" : "*",  
    "Effect" : "Allow"  
  }  
]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonHoneycodeTeamAssociationFullAccess

Description : Fournit un accès complet à Honeycode Team Association via le SDK Console de gestion AWS et le SDK.

AmazonHoneycodeTeamAssociationFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonHoneycodeTeamAssociationFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 juin 2020, 20:28 UTC
- Heure modifiée : 24 juin 2020, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonHoneycodeTeamAssociationReadOnlyAccess

Description : fournit un accès en lecture seule à Honeycode Team Association via le SDK Console de gestion AWS et le SDK.

AmazonHoneycodeTeamAssociationReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonHoneycodeTeamAssociationReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 24 juin 2020, 20:27 UTC
- Heure modifiée : 24 juin 2020, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonHoneycodeWorkbookFullAccess

Description : fournit un accès complet à Honeycode Workbook via le SDK Console de gestion AWS et le SDK.

AmazonHoneycodeWorkbookFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonHoneycodeWorkbookFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 juin 2020, 20:28 UTC
- Heure modifiée : 01 décembre 2020, 17:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonHoneycodeWorkbookReadOnlyAccess

Description : fournit un accès en lecture seule au classeur Honeycode via le SDK Console de gestion AWS et le SDK.

AmazonHoneycodeWorkbookReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonHoneycodeWorkbookReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 juin 2020, 20:28 UTC
- Heure modifiée : 01 décembre 2020, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonInspector2AgentlessServiceRolePolicy

Description : accorde à Amazon Inspector l'accès Services AWS nécessaire pour effectuer des évaluations de sécurité sans agent

AmazonInspector2AgentlessServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 20 novembre 2023, 15:18 UTC
- Heure modifiée : 20 août 2026, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  }
}

```

```
}  
]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonInspector2AmiScanServiceRolePolicy

Description : accorde à Amazon Inspector l'accès Services AWS nécessaire pour effectuer les évaluations de sécurité de l'AMI

AmazonInspector2AmiScanServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 30 juillet 2026, 17:57 UTC
- Heure modifiée : 30 juillet 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AmiScanServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonInspector2FullAccess

Description : fournit un accès complet à Amazon Inspector et à d'autres services connexes tels que les organisations.

AmazonInspector2FullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonInspector2FullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2021, 19:10 UTC
- Heure modifiée : 25 avril 2024, 13:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonInspector2FullAccess_v2

Description : fournit un accès complet à Amazon Inspector et à d'autres services connexes, tels que les organisations dont l'accès organisationnel est restreint.

AmazonInspector2FullAccess_v2 est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonInspector2FullAccess_v2` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 juillet 2025, 16:07 UTC
- Heure modifiée : 08 juillet 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess_v2`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonInspector2ManagedCisPolicy

Description : Il s'agit d'une politique gérée que le client doit associer à ses rôles pour communiquer avec le service d'inspection pour les scans CIS

AmazonInspector2ManagedCisPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonInspector2ManagedCisPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 janvier 2024, 16:31 UTC
- Heure modifiée : 24 janvier 2024, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
```

```
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonInspector2ManagedTelemetryPolicy

Description : accorde les autorisations nécessaires pour communiquer avec le canal de télémétrie Inspector2

AmazonInspector2ManagedTelemetryPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonInspector2ManagedTelemetryPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 février 2026, 17:12 UTC
- Heure modifiée : 13 février 2026, 17:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspector2ManagedTelemetryPolicy

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForInspector2Telemetry",
      "Effect" : "Allow",
      "Action" : [
        "inspector2-telemetry:StartSession",
        "inspector2-telemetry:StopSession",
        "inspector2-telemetry:SendTelemetry",
        "inspector2-telemetry:NotifyHeartbeat"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonInspector2ReadOnlyAccess

Description : Fournit un accès en lecture seule au service Amazon inspector2 et aux services de support pertinents

AmazonInspector2ReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonInspector2ReadOnlyAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 21 janvier 2022, 14:45 UTC
- Heure modifiée : 07 juillet 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonInspector2ServiceRolePolicy

Description : accorde à Amazon Inspector l'accès Services AWS nécessaire pour effectuer les évaluations de sécurité

AmazonInspector2ServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 16 novembre 2021, 20:27 UTC
- Heure modifiée : 16 juin 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy`

Version de la politique

Version de la politique : v27 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/D0-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"
            ]
        }
    }
}

```

```
}  
  }  
    }  
  ]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonInspector2ThirdPartyServiceRolePolicy

Description : autorise Amazon Inspector à effectuer des actions en votre nom dans le cadre de l'analyse des ressources multicloud.

AmazonInspector2ThirdPartyServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 26 juin 2026, 15:27 UTC
- Heure modifiée : 26 juin 2026, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ThirdPartyServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
      }
    }
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonInspectorFullAccess

Description : fournit un accès complet à Amazon Inspector.

AmazonInspectorFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonInspectorFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 octobre 2015, 17:08 UTC
- Heure modifiée : 21 décembre 2017, 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorFullAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonInspectorReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon Inspector.

AmazonInspectorReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonInspectorReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 07 octobre 2015, 17:08 UTC
- Heure modifiée : 01 octobre 2019, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonInspectorServiceRolePolicy

Description : accorde à Amazon Inspector l'accès Services AWS nécessaire pour effectuer les évaluations de sécurité

AmazonInspectorServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 21 novembre 2017, 15:48 UTC
- Heure modifiée : 11 septembre 2020, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonKendraFullAccess

Description : fournit un accès complet à Amazon Kendra via le Console de gestion AWS.

AmazonKendraFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonKendraFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 décembre 2019, 16:15 UTC
- Heure modifiée : 3 décembre 2019, 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonKendraReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon Kendra via le Console de gestion AWS.

AmazonKendraReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonKendraReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 décembre 2019, 16:13 UTC
- Heure modifiée : 27 mai 2021, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kendra:Describe*",
        "kendra:List*",
        "kendra:Query",
        "kendra:GetQuerySuggestions"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonKeyspacesFullAccess

Description : Fournissez un accès complet à Amazon Keyspaces

AmazonKeyspacesFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonKeyspacesFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 avril 2020, 17:06 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonKeyspacesReadOnlyAccess

Description : Fournir un accès en lecture seule à Amazon Keyspaces

AmazonKeyspacesReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonKeyspacesReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 avril 2020, 17:07 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonKeyspacesReadOnlyAccess_v2

Description : Fournissez un accès en lecture seule à Amazon Keyspaces et aux AWS services associés.

AmazonKeyspacesReadOnlyAccess_v2 est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonKeyspacesReadOnlyAccess_v2` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 septembre 2023, 17:01 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonKinesisAnalyticsFullAccess

Description : fournit un accès complet à Amazon Kinesis Analytics via le Console de gestion AWS.

AmazonKinesisAnalyticsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonKinesisAnalyticsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 21 septembre 2016, 19:01 UTC
- Heure modifiée : 21 septembre 2016, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonKinesisAnalyticsReadOnly

Description : fournit un accès en lecture seule à Amazon Kinesis Analytics via le. Console de gestion AWS

AmazonKinesisAnalyticsReadOnlyest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonKinesisAnalyticsReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 21 septembre 2016, 18:16 UTC
- Heure modifiée : 21 septembre 2016, 18:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonKinesisFirehoseFullAccess

Description : fournit un accès complet à tous les flux de diffusion Amazon Kinesis Firehose.

AmazonKinesisFirehoseFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonKinesisFirehoseFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 octobre 2015, 18:45 UTC
- Heure modifiée : 07 octobre 2015, 18:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "firehose:*"
      ],

```

```
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonKinesisFirehoseReadOnlyAccess

Description : fournit un accès en lecture seule à tous les flux de diffusion Amazon Kinesis Firehose.

AmazonKinesisFirehoseReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonKinesisFirehoseReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 octobre 2015, 18:43 UTC
- Heure modifiée : 07 octobre 2015, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonKinesisFullAccess

Description : Fournit un accès complet à tous les flux via le Console de gestion AWS.

AmazonKinesisFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonKinesisFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 06 février 2015, 18:40 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonKinesisReadOnlyAccess

Description : Fournit un accès en lecture seule à tous les flux via le Console de gestion AWS.

AmazonKinesisReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonKinesisReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 06 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonKinesisVideoStreamsFullAccess

Description : fournit un accès complet à Amazon Kinesis Video Streams via le Console de gestion AWS.

AmazonKinesisVideoStreamsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonKinesisVideoStreamsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2017, 23:27 UTC
- Heure modifiée : 01 décembre 2017, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonKinesisVideoStreamsReadOnlyAccess

Description : fournit un accès en lecture seule à AWS Kinesis Video Streams via le Console de gestion AWS.

AmazonKinesisVideoStreamsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonKinesisVideoStreamsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2017, 23:14 UTC
- Heure modifiée : 01 décembre 2017, 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
```



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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonLaunchWizard_Accès complet

Description : Accès complet à l'assistant de AWS lancement et aux autres services requis.

AmazonLaunchWizard_Fullaccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonLaunchWizard_Fullaccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 août 2020, 17:47 UTC
- Heure modifiée : 22 février 2023, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess`

Version de la politique

Version de la politique : v15 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonLaunchWizardFullAccessV2

Description : Accès complet à l'assistant de AWS lancement et aux autres services requis.

AmazonLaunchWizardFullAccessV2 est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonLaunchWizardFullAccessV2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 septembre 2023, 17:14 UTC
- Heure modifiée : 18 août 2026, 19:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*/*"
        }
      }
    }
  ]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonLexChannelsAccess

Description : Cette politique permet aux clients d'appeler Lex Runtime à partir de canaux

AmazonLexChannelsAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 13 janvier 2021, 20:12 UTC
- Heure modifiée : 13 janvier 2021, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexChannelsAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonLexFullAccess

Description : fournit un accès complet à Amazon Lex via le Console de gestion AWS. Permet également de créer des rôles liés au service Lex et d'accorder à Lex les autorisations nécessaires pour invoquer un ensemble limité de fonctions Lambda.

AmazonLexFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonLexFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 avril 2017, 23:20 UTC
- Heure modifiée : 16 avril 2024, 20:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexFullAccess`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"  
    ]  
  }  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonLexReadOnly

Description : fournit un accès en lecture seule à Amazon Lex.

AmazonLexReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonLexReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 avril 2017, 23:13 UTC
- Heure modifiée : 13 mai 2024, 16:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexReadOnly`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonLexReplicationPolicy

Description : permet à Amazon Lex de répliquer les ressources Lex dans différentes régions en votre nom.

AmazonLexReplicationPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 31 janvier 2024, 23:29 UTC
- Heure modifiée : 24 juin 2025, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            }
        }
    }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonLexRunBotsOnly

Description : Permet d'accéder aux API conversationnelles Amazon Lex.

AmazonLexRunBotsOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonLexRunBotsOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 avril 2017, 23:06 UTC
- Heure modifiée : 18 août 2021, 00:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexRunBotsOnly`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonLexV2BotPolicy

Description : permet aux robots Lex V2 d'accéder à d'autres AWS services en votre nom.

AmazonLexV2BotPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 13 janvier 2021, 20:10 UTC
- Heure modifiée : 13 janvier 2021, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonLookoutEquipmentFullAccess

Description : fournit un accès complet à Amazon Lookout pour les opérations relatives à l'équipement

AmazonLookoutEquipmentFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonLookoutEquipmentFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 08 avril 2021, 15:52 UTC
- Heure modifiée : 24 novembre 2021, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonLookoutEquipmentReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon Lookout for Equipments

AmazonLookoutEquipmentReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonLookoutEquipmentReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 mai 2021, 16:47 UTC
- Heure modifiée : 10 novembre 2022, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonLookoutMetricsFullAccess

Description : donne accès à toutes les actions d'Amazon Lookout for Metrics

AmazonLookoutMetricsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonLookoutMetricsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 mai 2021, 00:43 UTC
- Heure modifiée : 07 mai 2021, 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonLookoutMetricsReadOnlyAccess

Description : donne accès à toutes les actions en lecture seule pour Amazon Lookout for Metrics

AmazonLookoutMetricsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonLookoutMetricsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 mai 2021, 00:43 UTC
- Heure modifiée : 04 janvier 2022, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonLookoutVisionConsoleFullAccess

Description : fournit un accès complet à Amazon Lookout for Vision et un accès limité aux dépendances de service et de console requises.

AmazonLookoutVisionConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonLookoutVisionConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 mai 2021, 19:37 UTC
- Heure modifiée : 11 mai 2021, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonLookoutVisionConsoleReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon Lookout for Vision et un accès limité aux dépendances de service et de console requises.

AmazonLookoutVisionConsoleReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonLookoutVisionConsoleReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 mai 2021, 19:32 UTC
- Heure modifiée : 09 décembre 2021, 02:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonLookoutVisionFullAccess

Description : fournit un accès complet à Amazon Lookout for Vision et un accès limité aux dépendances requises.

AmazonLookoutVisionFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonLookoutVisionFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 mai 2021, 19:24 UTC
- Heure modifiée : 11 mai 2021, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonLookoutVisionReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon Lookout for Vision et un accès limité aux dépendances requises.

AmazonLookoutVisionReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonLookoutVisionReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 mai 2021, 19:11 UTC

- Heure modifiée : 09 décembre 2021, 03:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMachineLearningBatchPredictionsAccess

Description : autorise les utilisateurs à demander des prévisions par lots Amazon Machine Learning.

AmazonMachineLearningBatchPredictionsAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMachineLearningBatchPredictionsAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 avril 2015, 17:12 UTC
- Heure modifiée : 09 avril 2015, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning>DeleteBatchPrediction",
```

```
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
        "machinelearning:UpdateBatchPrediction"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMachineLearningCreateOnlyAccess

Description : permet de créer un accès aux ressources Amazon Machine Learning sans prédiction.

AmazonMachineLearningCreateOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMachineLearningCreateOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 avril 2015, 17:18 UTC
- Heure modifiée : 29 juin 2016, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning>Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMachineLearningFullAccess

Description : fournit un accès complet aux ressources Amazon Machine Learning.

AmazonMachineLearningFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMachineLearningFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 avril 2015, 17:25 UTC
- Heure modifiée : 09 avril 2015, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

Description : accorde aux utilisateurs l'autorisation de créer et de supprimer le point de terminaison en temps réel pour les modèles Amazon Machine Learning.

AmazonMachineLearningManageRealTimeEndpointOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMachineLearningManageRealTimeEndpointOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 avril 2015, 17:32 UTC
- Heure modifiée : 09 avril 2015, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningManageRealTimeEndpointOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateRealtimeEndpoint",
        "machinelearning>DeleteRealtimeEndpoint"
      ]
    }
  ],
}
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMachineLearningReadOnlyAccess

Description : fournit un accès en lecture seule aux ressources Amazon Machine Learning.

AmazonMachineLearningReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMachineLearningReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 avril 2015, 17:40 UTC
- Heure modifiée : 09 avril 2015, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMachineLearningRealTimePredictionOnlyAccess

Description : autorise les utilisateurs à demander des prévisions en temps réel à Amazon Machine Learning.

AmazonMachineLearningRealTimePredictionOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMachineLearningRealTimePredictionOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 avril 2015, 17:44 UTC

- Heure modifiée : 09 avril 2015, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningRealTimePredictionOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMachineLearningRoleforRedshiftDataSourceV3

Description : permet à Machine Learning de configurer et d'utiliser vos clusters Redshift et vos emplacements de stockage S3 pour la source de données Redshift.

AmazonMachineLearningRoleforRedshiftDataSourceV3 est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMachineLearningRoleforRedshiftDataSourceV3 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 24 juin 2020, 18:00 UTC
- Heure modifiée : 24 juin 2020, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMacieFullAccess

Description : fournit un accès complet à Amazon Macie.

AmazonMacieFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMacieFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 14 août 2017, 14:54 UTC
- Heure modifiée : 01 juillet 2022, 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieFullAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMacieHandshakeRole

Description : accorde l'autorisation de créer le rôle lié à un service d'Amazon Macie.

AmazonMacieHandshakeRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMacieHandshakeRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 28 juin 2018, 15:46 UTC
- Heure modifiée : 28 juin 2018, 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "iam:AWSServiceName" : "macie.amazonaws.com"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMacieReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon Macie.

AmazonMacieReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMacieReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 juin 2023, 21:50 UTC
- Heure modifiée : 15 juin 2023, 21:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:SearchResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMacieServiceRole

Description : accorde à Macie un accès en lecture seule aux dépendances des ressources de votre compte afin de permettre l'analyse des données.

AmazonMacieServiceRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMacieServiceRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 14 août 2017, 14:53 UTC
- Heure modifiée : 14 août 2017, 14:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMacieServiceRolePolicy

Description : rôle lié à un service pour Amazon Macie

AmazonMacieServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 19 juin 2018, 22:17 UTC
- Heure modifiée : 19 mai 2022, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMacieServiceRolePolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/maciek/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:PutLogEvents",
      "logs:DescribeLogStreams"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/maciek/*:log-stream:*"
    ]
  }

```

```
}  
]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonManagedBlockchainConsoleFullAccess

Description : Fournit un accès complet à Amazon Managed Blockchain via le Console de gestion AWS

AmazonManagedBlockchainConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonManagedBlockchainConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 avril 2019, 21:23 UTC
- Heure modifiée : 29 avril 2019, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonManagedBlockchainFullAccess

Description : fournit un accès complet à Amazon Managed Blockchain.

AmazonManagedBlockchainFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonManagedBlockchainFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 avril 2019, 21:39 UTC
- Heure modifiée : 29 avril 2019, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonManagedBlockchainReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon Managed Blockchain.

AmazonManagedBlockchainReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonManagedBlockchainReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 avril 2019, 18:17 UTC
- Heure modifiée : 30 avril 2019, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
        " * "
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonManagedBlockchainServiceRolePolicy

Description : Permet l'accès aux ressources utilisées ou gérées par Amazon Managed Blockchain Services AWS et aux ressources utilisées ou gérées par celle-ci

AmazonManagedBlockchainServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 17 janvier 2020, 19:51 UTC
- Heure modifiée : 17 janvier 2020, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMCSFullAccess

Description : Fournir un accès complet au service Amazon Managed Apache Cassandra

AmazonMCSFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonMCSFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 décembre 2019, 13:45 UTC
- Heure modifiée : 17 avril 2020, 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMCSReadOnlyAccess

Description : Fournir un accès en lecture seule au service Amazon Managed Apache Cassandra

AmazonMCSReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMCSReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 décembre 2019, 13:46 UTC
- Heure modifiée : 17 avril 2020, 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMechanicalTurkFullAccess

Description : fournit un accès complet à toutes les API d'Amazon Mechanical Turk.

AmazonMechanicalTurkFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMechanicalTurkFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 décembre 2015, 19:08 UTC
- Heure modifiée : 11 décembre 2015, 19:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMechanicalTurkReadOnly

Description : permet d'accéder aux API en lecture seule d'Amazon Mechanical Turk.

AmazonMechanicalTurkReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMechanicalTurkReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 décembre 2015, 19:08 UTC
- Heure modifiée : 25 septembre 2019, 21:06 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkReadOnly`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMemoryDBFullAccess

Description : fournit un accès complet à Amazon MemoryDB via le. Console de gestion AWS

AmazonMemoryDBFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMemoryDBFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 octobre 2021, 19:24 UTC
- Heure modifiée : 08 octobre 2021, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

```
}  
  }  
  ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMemoryDBReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon MemoryDB via le. Console de gestion AWS

AmazonMemoryDBReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMemoryDBReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 octobre 2021, 19:27 UTC
- Heure modifiée : 08 octobre 2021, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMobileAnalyticsFinancialReportAccess

Description : fournit un accès en lecture seule à tous les rapports, y compris les données financières pour toutes les ressources de l'application.

AmazonMobileAnalyticsFinancialReportAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMobileAnalyticsFinancialReportAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 06 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFinancialReportAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMobileAnalyticsFullAccess

Description : fournit un accès complet à toutes les ressources de l'application.

AmazonMobileAnalyticsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMobileAnalyticsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 06 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMobileAnalyticsNon-financialReportAccess

Description : fournit un accès en lecture seule aux rapports non financiers pour toutes les ressources de l'application.

AmazonMobileAnalyticsNon-financialReportAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMobileAnalyticsNon-financialReportAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 06 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMobileAnalyticsWriteOnlyAccess

Description : fournit un accès en écriture seule aux données d'événement put pour toutes les ressources de l'application. (Recommandé pour l'intégration du SDK)

AmazonMobileAnalyticsWriteOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMobileAnalyticsWriteOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 06 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMonitronFullAccess

Description : fournit un accès complet à la gestion d'Amazon Monitron

AmazonMonitronFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMonitronFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 décembre 2020, 22:40 UTC
- Heure modifiée : 08 juin 2022, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMonitronFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMQApiFullAccess

Description : fournit un accès complet à AmazonMQ via notre API/SDK

AmazonMQApiFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMQApiFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 décembre 2018, 20:31 UTC
- Heure modifiée : 04 novembre 2020, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMQApiReadOnlyAccess

Description : fournit un accès en lecture seule à AmazonMQ via notre API/SDK

AmazonMQApiReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMQApiReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 décembre 2018, 20:31 UTC
- Heure modifiée : 18 décembre 2018, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMQFullAccess

Description : fournit un accès complet à AmazonMQ via le. Console de gestion AWS

AmazonMQFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMQFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2017, 15:28 UTC
- Heure modifiée : 03 septembre 2026, 22:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQFullAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
                ]
            }
        }
    }
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMQReadOnlyAccess

Description : fournit un accès en lecture seule à AmazonMQ via le. Console de gestion AWS

AmazonMQReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMQReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2017, 15:30 UTC
- Heure modifiée : 28 novembre 2017, 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMQServiceRolePolicy

Description : Politique relative aux rôles liés aux services pour AWS Amazon MQ

AmazonMQServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 04 novembre 2020, 16:07 UTC
- Heure modifiée : 04 novembre 2020, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMSKConnectReadOnlyAccess

Description : Fournir un accès en lecture seule à Amazon MSK Connect

AmazonMSKConnectReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonMSKConnectReadOnlyAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 septembre 2021, 10:18 UTC
- Heure modifiée : 18 octobre 2021, 09:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMSKFullAccess

Description : Fournissez un accès complet à Amazon MSK et aux autres autorisations requises pour ses dépendances.

AmazonMSKFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMSKFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 janvier 2019, 22:07 UTC
- Heure modifiée : 18 octobre 2023, 11:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMSKFullAccess

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  }
}
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMSKReadOnlyAccess

Description : Fournir un accès en lecture seule à Amazon MSK

AmazonMSKReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonMSKReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 janvier 2019, 22:28 UTC
- Heure modifiée : 14 janvier 2019, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMWAAServerlessServiceRolePolicy

Description : Permet d'accéder au service Amazon Airflow Serverless pour gérer la mise en réseau de vos flux de travail et accéder à d'autres AWS services en votre nom

AmazonMWAAServerlessServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 15 novembre 2025, 20:34 UTC
- Heure modifiée : 15 novembre 2025, 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServerlessServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonMWAAServiceRolePolicy

Description : rôle lié au service utilisé par Amazon Managed Workflows pour Apache Airflow.

AmazonMWAAServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 24 novembre 2020, 14:13 UTC
- Heure modifiée : 17 novembre 2022, 00:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  ]
}
}
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonNimbleStudio-LaunchProfileWorker

Description : Cette politique donne accès aux ressources nécessaires aux employés de Nimble Studio Launch Profile. Associez cette politique aux instances EC2 créées par Nimble Studio Builder.

AmazonNimbleStudio-LaunchProfileWorker est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonNimbleStudio-LaunchProfileWorker à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 avril 2021, 04:47 UTC
- Heure modifiée : 28 avril 2021, 04:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonNimbleStudio-StudioAdmin

Description : Cette politique donne accès aux ressources Amazon Nimble Studio associées à l'administrateur du studio et aux ressources de studio associées dans d'autres services. Associez cette politique au rôle d'administrateur associé à votre studio.

AmazonNimbleStudio-StudioAdmin est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonNimbleStudio-StudioAdmin à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 avril 2021, 04:47 UTC
- Heure modifiée : 22 septembre 2023, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonNimbleStudio-StudioUser

Description : Cette politique donne accès aux ressources Amazon Nimble Studio associées à l'utilisateur du studio et aux ressources de studio associées dans d'autres services. Associez cette politique au rôle d'utilisateur associé à votre studio.

AmazonNimbleStudio-StudioUser est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonNimbleStudio-StudioUser à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 avril 2021, 04:48 UTC
- Heure modifiée : 22 septembre 2023, 17:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonODBAutonomousDatabaseAdmin

Description : fournit un accès administratif pour gérer les ressources de base de données autonomes dans Oracle Database@AWS.

AmazonODBAutonomousDatabaseAdmin est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonODBAutonomousDatabaseAdmin à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux fonctions du poste
- Heure de création : 04 septembre 2026, 21:47 UTC

- Heure modifiée : 04 septembre 2026, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AmazonODBAutonomousDatabaseAdmin`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonODBAutonomousVmClusterAdmin

Description : fournit un accès administratif pour gérer les ressources du cluster de machines virtuelles autonomes dans Oracle Database@AWS

AmazonODBAutonomousVmClusterAdmin est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonODBAutonomousVmClusterAdmin à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux fonctions
- Heure de création : 07 août 2026, 01:12 UTC

- Heure modifiée : 04 septembre 2026, 21:17 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AmazonODBAutonomousVmClusterAdmin`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonODBExadataInfrastructureAdmin

Description : fournit un accès administratif pour gérer les ressources de l'infrastructure Exadata dans Oracle Database@AWS

AmazonODBExadataInfrastructureAdmin est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonODBExadataInfrastructureAdmin à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux fonctions
- Heure de création : 07 août 2026, 01:12 UTC
- Heure modifiée : 04 septembre 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AmazonODBExadataInfrastructureAdmin`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonODBExadataVmClusterAdmin

Description : fournit un accès administratif pour gérer les ressources du cluster de machines virtuelles Exadata dans Oracle AWS Database@.

AmazonODBExadataVmClusterAdmin est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonODBExadataVmClusterAdmin à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux fonctions
- Heure de création : 04 septembre 2026, 21:37 UTC
- Heure modifiée : 04 septembre 2026, 21:37 UTC
- ARN: arn:aws:iam::aws:policy/job-function/AmazonODBExadataVmClusterAdmin

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonODBExascaleStorageVaultAdmin

Description : fournit un accès administratif pour gérer les ressources du coffre-fort de stockage Exascale dans Oracle Database@.AWS

Amazon0DBExascaleStorageVaultAdminest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer Amazon0DBExascaleStorageVaultAdmin à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux fonctions
- Heure de création : 04 septembre 2026, 21:37 UTC
- Heure modifiée : 04 septembre 2026, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/Amazon0DBExascaleStorageVaultAdmin`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonODBExascaleVmClusterAdmin

Description : fournit un accès administratif pour gérer les ressources du cluster de machines virtuelles Exascale dans Oracle Database@.AWS

AmazonODBExascaleVmClusterAdminest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonODBExascaleVmClusterAdmin à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux fonctions
- Heure de création : 04 septembre 2026, 21:37 UTC
- Heure modifiée : 04 septembre 2026, 21:37 UTC
- ARN: arn:aws:iam::aws:policy/job-function/AmazonODBExascaleVmClusterAdmin

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonODBFullAccess

Description : fournit un accès complet aux ressources d'Oracle Database@AWS

AmazonODBFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonODBFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 juillet 2026, 22:57 UTC
- Heure modifiée : 04 septembre 2026, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonODBFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            ]
        }
    }
}
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonODBNetworkAdmin

Description : fournit un accès administratif aux ressources réseau pour Oracle Database@AWS

AmazonODBNetworkAdmin est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonODBNetworkAdmin à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux fonctions
- Heure de création : 07 août 2026, 01:12 UTC
- Heure modifiée : 04 septembre 2026, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AmazonODBNetworkAdmin`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonODBReadOnlyAccess

Description : fournit un accès en lecture seule aux ressources Oracle Database@AWS

Amazon0DBReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer Amazon0DBReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 août 2026, 01:12 UTC
- Heure modifiée : 04 septembre 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/Amazon0DBReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonODBSERVICERolePolicy

Description : Permet à Oracle Database@AWS de gérer les AWS ressources en votre nom.

AmazonODBSERVICERolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 13 novembre 2024, 18:21 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonODBSERVICERolePolicy`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonOmicsFullAccess

Description : fournit un accès complet à Amazon Omics et à d'autres fonctionnalités requises Services AWS. Cette politique permet à l'utilisateur de consulter et d'accepter les invitations de partage de RAM pour accéder à des ressources extérieures à celles de l'utilisateur Compte AWS.

AmazonOmicsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonOmicsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 février 2023, 00:59 UTC
- Heure modifiée : 24 février 2023, 00:59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOmicsFullAccess

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonOmicsReadOnlyAccess

Description : Fournir un accès en lecture seule à Amazon Omics

AmazonOmicsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonOmicsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2022, 04:17 UTC
- Heure modifiée : 29 novembre 2022, 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonOneEnterpriseFullAccess

Description : Cette politique accorde des autorisations administratives qui permettent d'accéder à toutes les ressources et opérations d'Amazon One Enterprise.

AmazonOneEnterpriseFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonOneEnterpriseFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2023, 04:58 UTC

- Heure modifiée : 28 novembre 2023, 04:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonOneEnterpriseInstallerAccess

Description : Cette politique accorde des autorisations de lecture et d'écriture limitées qui permettent l'installation et l'activation de l'appareil.

AmazonOneEnterpriseInstallerAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonOneEnterpriseInstallerAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2023, 05:00 UTC
- Heure modifiée : 28 novembre 2023, 05:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstallerAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:CreateDeviceActivationQrCode",
        "one:GetDeviceInstance",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceInstances",
        "one:ListSites"
      ],
      "Resource" : "*"
    }
  ]
}
```



```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonOneEnterpriseReadOnlyAccess

Description : Cette politique accorde des autorisations en lecture seule à toutes les ressources et opérations d'Amazon One Enterprise.

AmazonOneEnterpriseReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonOneEnterpriseReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2023, 04:59 UTC
- Heure modifiée : 28 novembre 2023, 04:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonOpenSearchDashboardsServiceRolePolicy

Description : Permet d'accéder à Amazon OpenSearch Dashboards Service pour accéder à d'autres AWS services, par exemple CloudWatch en votre nom

AmazonOpenSearchDashboardsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle

- Heure de création : 22 décembre 2023, 19:38 UTC
- Heure modifiée : 22 décembre 2023, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonOpenSearchDirectQueryGlueCreateAccess

Description : permet au OpenSearch DirectQuery Service d'accéder aux API AWS Glue pour créer des ressources en votre nom.

AmazonOpenSearchDirectQueryGlueCreateAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonOpenSearchDirectQueryGlueCreateAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 mai 2024, 12:24 UTC
- Heure modifiée : 06 mai 2024, 12:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchDirectQueryGlueCreateAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonOpenSearchDirectQueryGlueCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:CreatePartition",
```

```
        "glue:CreateTable",
        "glue:BatchCreatePartition"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonOpenSearchIngestionFullAccess

Description : permet à Amazon OpenSearch Ingestion d'accéder à d'autres AWS services en votre nom.

AmazonOpenSearchIngestionFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonOpenSearchIngestionFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 avril 2023, 18:11 UTC
- Heure modifiée : 26 avril 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonOpenSearchIngestionReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon OpenSearch Ingestion Service

AmazonOpenSearchIngestionReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonOpenSearchIngestionReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 avril 2023, 18:09 UTC
- Heure modifiée : 26 avril 2023, 18:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "osis:GetPipeline",
      "osis:GetPipelineChangeProgress",
      "osis:GetPipelineBlueprint",
      "osis:ListPipelineBlueprints",
      "osis:ListPipelines",
      "osis:ListTagsForResource"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonOpenSearchIngestionServiceRolePolicy

Description : permet à Amazon OpenSearch Ingestion Service d'accéder à d'autres AWS services en votre nom.

AmazonOpenSearchIngestionServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 18 novembre 2022, 16:49 UTC

- Heure modifiée : 28 août 2025, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
```

```
}  
  }  
  ]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonOpenSearchServerlessServiceRolePolicy

Description : Autorisez Amazon OpenSearch Serverless à accéder à d'autres AWS services tels que CloudWatch des API en votre nom.

AmazonOpenSearchServerlessServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 24 novembre 2022, 19:50 UTC
- Heure modifiée : 25 juillet 2024, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonOpenSearchServiceCognitoAccess

Description : Permet d'accéder au service de configuration Amazon Cognito.

AmazonOpenSearchServiceCognitoAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonOpenSearchServiceCognitoAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 septembre 2021, 06:31 UTC

- Heure modifiée : 20 décembre 2021, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonOpenSearchServiceFullAccess

Description : fournit un accès complet au OpenSearch service de configuration Amazon Service.

AmazonOpenSearchServiceFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonOpenSearchServiceFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 septembre 2021, 05:33 UTC

- Heure modifiée : 08 septembre 2021, 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonOpenSearchServiceReadOnlyAccess

Description : fournit un accès en lecture seule au service de configuration Amazon OpenSearch Service.

AmazonOpenSearchServiceReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonOpenSearchServiceReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 septembre 2021, 05:38 UTC
- Heure modifiée : 08 septembre 2021, 05:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonOpenSearchServiceRolePolicy

Description : Autorisez Amazon OpenSearch Service à accéder à d'autres AWS services tels que les API réseau EC2 en votre nom.

AmazonOpenSearchServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 26 août 2021, 09:27 UTC
- Heure modifiée : 27 mars 2025, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
      }
    }
  ]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonPersonalizeFullAccess

Description : fournit un accès complet à Amazon Personalize via le SDK Console de gestion AWS et. Fournit également un accès sélectif à des services connexes (par exemple, S3, CloudWatch).

AmazonPersonalizeFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonPersonalizeFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 04 décembre 2018, 22:24 UTC
- Heure modifiée : 30 mai 2019, 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonPollyFullAccess

Description : accorde un accès complet au service et aux ressources Amazon Polly.

AmazonPollyFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonPollyFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 novembre 2016, 18:59 UTC
- Heure modifiée : 30 novembre 2016, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonPollyReadOnlyAccess

Description : accorde un accès en lecture seule aux ressources Amazon Polly.

AmazonPollyReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonPollyReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 novembre 2016, 18:59 UTC
- Heure modifiée : 01 avril 2026, 08:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "polly:DescribeVoices",
      "polly:GetLexicon",
      "polly:GetSpeechSynthesisTask",
      "polly:ListLexicons",
      "polly:ListSpeechSynthesisTasks",
      "polly:SynthesizeSpeech",
      "polly:StartSpeechSynthesisStream"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonPrometheusConsoleFullAccess

Description : accorde un accès complet aux ressources AWS gérées de Prometheus dans la console AWS

AmazonPrometheusConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonPrometheusConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 décembre 2020, 18:11 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonPrometheusFullAccess

Description : Donne un accès complet aux ressources AWS gérées de Prometheus

AmazonPrometheusFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonPrometheusFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 décembre 2020, 18:10 UTC
- Heure modifiée : 26 novembre 2023, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/scrapper.aps.amazonaws.com/
AWSServiceRoleForAmazonPrometheusScrapper*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "scrapper.aps.amazonaws.com"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonPrometheusQueryAccess

Description : donne accès à l'exécution de requêtes sur les ressources AWS gérées de Prometheus

AmazonPrometheusQueryAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonPrometheusQueryAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 19 décembre 2020, 01:02 UTC
- Heure modifiée : 19 décembre 2020, 01:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonPrometheusRemoteWriteAccess

Description : accorde un accès en écriture uniquement aux espaces de travail Prometheus AWS gérés

AmazonPrometheusRemoteWriteAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonPrometheusRemoteWriteAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 décembre 2020, 01:04 UTC
- Heure modifiée : 19 décembre 2020, 01:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonPrometheusScrapperServiceRolePolicy

Description : Permet d'accéder aux AWS ressources gérées ou utilisées par Amazon Managed Service pour Prometheus Collector

AmazonPrometheusScrapperServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 26 novembre 2023, 14:19 UTC
- Heure modifiée : 17 juillet 2026, 08:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScrapperServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeleteSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scrapper.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScrapper*"
    },
    {
      "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" : [
            "AMPAgentlessScrapper"
          ]
        }
      }
    },
    {
      "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}"
      }
    }
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonQDeveloperAccess

Description : fournit un accès aux développeurs pour leur permettre d'interagir avec Amazon Q

AmazonQDeveloperAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonQDeveloperAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 juillet 2024, 08:35 UTC
- Heure modifiée : 20 mai 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQDeveloperAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonQFullAccess

Description : fournit un accès complet pour permettre les interactions avec Amazon Q

AmazonQFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonQFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2023, 16:00 UTC
- Heure modifiée : 20 mai 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQFullAccess`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            ]
        }
    }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonQLDBConsoleFullAccess

Description : fournit un accès complet à Amazon QLDB via le. Console de gestion AWS

AmazonQLDBConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonQLDBConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 septembre 2019, 18:24 UTC
- Heure modifiée : 04 novembre 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}

```

```
}  
  }  
  ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonQLDBFullAccess

Description : fournit un accès complet à Amazon QLDB via l'API du service.

AmazonQLDBFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonQLDBFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 septembre 2019, 18:23 UTC
- Heure modifiée : 04 novembre 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBFullAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonQLDBReadOnly

Description : fournit un accès en lecture seule à Amazon QLDB.

AmazonQLDBReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonQLDBReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 septembre 2019, 18:19 UTC
- Heure modifiée : 02 juillet 2021, 02:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQLDBReadOnly

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRDSBetaServiceRolePolicy

Description : permet à Amazon RDS de gérer les AWS ressources en votre nom.

AmazonRDSBetaServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 02 mai 2018, 19:41 UTC
- Heure modifiée : 07 août 2024, 00:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSBetaServiceRolePolicy`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            }
        }
    }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRDSCustomInstanceProfileRolePolicy

Description : Permet à Amazon RDS Custom d'effectuer diverses actions d'automatisation et tâches de gestion de base de données via un profil d'instance EC2.

AmazonRDSCustomInstanceProfileRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRDSCustomInstanceProfileRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 février 2024, 17:42 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRDSCustomPreviewServiceRolePolicy

Description : Politique relative aux rôles du service de prévisualisation personnalisée Amazon RDS

AmazonRDSCustomPreviewServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 08 octobre 2021, 21:44 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy`

Version de la politique

Version de la politique : v15 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
}
```

```
]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRDSCustomServiceRolePolicy

Description : permet à Amazon RDS Custom de gérer les AWS ressources en votre nom.

AmazonRDSCustomServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 08 octobre 2021, 21:39 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy`

Version de la politique

Version de la politique : v19 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRDSDDataFullAccess

Description : Permet un accès complet à l'utilisation des API de données RDS, des API de stockage secret pour les informations d'identification de la base de données RDS et des API de gestion des requêtes de la console de base de données pour exécuter des instructions SQL sur des clusters Aurora Serverless dans le Compte AWS.

AmazonRDSDDataFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRDSDDataFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 novembre 2018, 21:29 UTC
- Heure modifiée : 20 novembre 2019, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSDDataFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRDSDirectoryServiceAccess

Description : Autorisez RDS à accéder à Directory Service Managed AD au nom du client pour les instances de bases de données SQL Server jointes à un domaine.

AmazonRDSDirectoryServiceAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRDSDirectoryServiceAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 26 février 2016, 02:02 UTC
- Heure modifiée : 15 mai 2019, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
    }
  ]
}
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRDSEnhancedMonitoringRole

Description : Donne accès à Cloudwatch pour la surveillance améliorée RDS

AmazonRDSEnhancedMonitoringRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRDSEnhancedMonitoringRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 11 novembre 2015, 19:58 UTC
- Heure modifiée : 11 novembre 2015, 19:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRDSFullAccess

Description : fournit un accès complet à Amazon RDS via le Console de gestion AWS.

AmazonRDSFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRDSFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 17 août 2023, 23:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSFullAccess`

Version de la politique

Version de la politique : v14 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRDSPerformanceInsightsFullAccess

Description : fournit un accès complet à RDS Performance Insights via le Console de gestion AWS

AmazonRDSPerformanceInsightsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonRDSPerformanceInsightsFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 août 2023, 23:41 UTC
- Heure modifiée : 23 juillet 2026, 00:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "AmazonRDSPerformanceInsightsAnalysisReportFullAccess",
```

```

    "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" : "*"
}

```

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRDSPerformanceInsightsReadOnly

Description : Read-Only politique pour RDS Performance Insights

AmazonRDSPerformanceInsightsReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRDSPerformanceInsightsReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 avril 2022, 00:02 UTC
- Heure modifiée : 22 juillet 2026, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"  
    }  
  ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRDSPreviewServiceRolePolicy

Description : Politique relative aux rôles du service Amazon RDS Preview

AmazonRDSPreviewServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 31 mai 2018, 18:02 UTC
- Heure modifiée : 07 août 2024, 01:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"  
    }  
  }  
}  
]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRDSReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon RDS via le Console de gestion AWS.

AmazonRDSReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRDSReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 14 avril 2023, 12:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRDSServiceRolePolicy

Description : permet à Amazon RDS de gérer les AWS ressources en votre nom.

AmazonRDSServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 08 janvier 2018, 18:17 UTC
- Heure modifiée : 01 juillet 2024, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy`

Version de la politique

Version de la politique : v14 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRedshiftAllCommandsFullAccess

Description : Cette politique inclut l'autorisation d'exécuter des commandes SQL pour copier, charger, télécharger, interroger et analyser des données sur Amazon Redshift. La politique accorde également l'autorisation d'exécuter certaines déclarations pour des services connexes, tels qu'Amazon S3, Amazon CloudWatch logs SageMaker, Amazon ou AWS Glue.

AmazonRedshiftAllCommandsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRedshiftAllCommandsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 novembre 2021, 00:48 UTC
- Heure modifiée : 25 novembre 2021, 02:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
          ]
        }
      }
    }
  ]
}

```


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRedshiftDataFullAccess

Description : Cette politique fournit un accès complet aux API Amazon Redshift Data. Cette politique accorde également un accès limité aux autres services requis.

AmazonRedshiftDataFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRedshiftDataFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 septembre 2020, 19:23 UTC
- Heure modifiée : 07 avril 2023, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRedshiftFederatedAuthorization

Description : Il s'agit d'une politique de facilité d'utilisation pour exécuter des requêtes avec Amazon Redshift Federated Authorization

AmazonRedshiftFederatedAuthorization est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRedshiftFederatedAuthorization à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 novembre 2025, 00:04 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftFederatedAuthorization`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRedshiftFullAccess

Description : fournit un accès complet à Amazon Redshift via le Console de gestion AWS.

AmazonRedshiftFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRedshiftFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 07 juillet 2022, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRedshiftQueryEditor

Description : fournit un accès complet à l'éditeur de requêtes Amazon Redshift et aux requêtes enregistrées via le Console de gestion AWS.

AmazonRedshiftQueryEditor est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRedshiftQueryEditor à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 octobre 2018, 22:50 UTC
- Heure modifiée : 16 février 2021, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
  }
}
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRedshiftQueryEditorV2FullAccess

Description : accorde un accès complet aux opérations et aux ressources d'Amazon Redshift Query Editor V2. Cette politique permet également d'accéder à d'autres services requis. Cela inclut les autorisations nécessaires pour répertorier les clusters Amazon Redshift, lire les clés et les alias dans AWS KMS et gérer les secrets de l'éditeur de requêtes V2 dans AWS Secrets Manager.

AmazonRedshiftQueryEditorV2FullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRedshiftQueryEditorV2FullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 septembre 2021, 14:06 UTC
- Heure modifiée : 21 février 2024, 17:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRedshiftQueryEditorV2NoSharing

Description : permet de travailler avec Amazon Redshift Query Editor V2 sans partager de ressources. Le mandant autorisé peut uniquement lire, mettre à jour et supprimer ses propres ressources mais ne peut pas les partager. Cette politique permet également d'accéder à d'autres services requis. Cela inclut les autorisations nécessaires pour répertorier les clusters Amazon Redshift et gérer les secrets Query Editor V2 du principal dans AWS Secrets Manager.

AmazonRedshiftQueryEditorV2NoSharingest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRedshiftQueryEditorV2NoSharing à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 septembre 2021, 14:18 UTC
- Heure modifiée : 21 février 2024, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
  }
}
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRedshiftQueryEditorV2ReadSharing

Description : permet de travailler avec Amazon Redshift Query Editor V2 avec un partage limité des ressources. Le principal bénéficiaire peut lire, écrire et partager ses propres ressources. Le principal autorisé peut lire les ressources partagées avec son équipe mais ne peut pas les mettre à jour.

Cette politique permet également d'accéder à d'autres services requis. Cela inclut les autorisations nécessaires pour répertorier les clusters Amazon Redshift et gérer les secrets Query Editor V2 du principal dans AWS Secrets Manager.

AmazonRedshiftQueryEditorV2ReadSharingest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRedshiftQueryEditorV2ReadSharing à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 septembre 2021, 14:22 UTC
- Heure modifiée : 21 février 2024, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:user}"
        }
    }
},
{
    "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}"
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRedshiftQueryEditorV2ReadWriteSharing

Description : permet de travailler avec Amazon Redshift Query Editor V2 en partageant les ressources. Le principal bénéficiaire peut lire, écrire et partager ses propres ressources. Le principal autorisé peut lire et mettre à jour les ressources partagées avec son équipe. Cette politique permet également d'accéder à d'autres services requis. Cela inclut les autorisations nécessaires pour répertorier les clusters Amazon Redshift et gérer les secrets Query Editor V2 du principal dans AWS Secrets Manager.

AmazonRedshiftQueryEditorV2ReadWriteSharing est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRedshiftQueryEditorV2ReadWriteSharing à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 septembre 2021, 14:25 UTC
- Heure modifiée : 21 février 2024, 17:30 UTC

- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRedshiftReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon Redshift via le Console de gestion AWS.

AmazonRedshiftReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRedshiftReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 08 février 2024, 00:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRedshiftServiceLinkedRolePolicy

Description : Permet à Amazon Redshift d'appeler les AWS services en votre nom

AmazonRedshiftServiceLinkedRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 18 septembre 2017, 19:19 UTC
- Heure modifiée : 19 février 2025, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy`

Version de la politique

Version de la politique : v15 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRekognitionCustomLabelsFullAccess

Description : Cette politique spécifie les autorisations Rekognition et s3 requises par la fonctionnalité Amazon Rekognition Custom Labels.

AmazonRekognitionCustomLabelsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRekognitionCustomLabelsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 janvier 2020, 19:18 UTC
- Heure modifiée : 16 août 2022, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]

```



```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRekognitionFullAccess

Description : Accès à toutes les API Amazon Rekognition

AmazonRekognitionFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRekognitionFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 novembre 2016, 14:40 UTC
- Heure modifiée : 30 novembre 2016, 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRekognitionReadOnlyAccess

Description : Accès à toutes les API de reconnaissance de lecture

AmazonRekognitionReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRekognitionReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 novembre 2016, 14:58 UTC
- Heure modifiée : 08 novembre 2023, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRekognitionServiceRole

Description : Permet à Rekognition d'appeler les AWS services en votre nom.

AmazonRekognitionServiceRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRekognitionServiceRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 29 novembre 2017, 16:52 UTC
- Heure modifiée : 29 novembre 2017, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRoute53AutoNamingFullAccess

Description : fournit un accès complet à toutes les actions de dénomination automatique de Route 53.

AmazonRoute53AutoNamingFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRoute53AutoNamingFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 janvier 2018, 18:40 UTC
- Heure modifiée : 18 janvier 2018, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
    "*"
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRoute53AutoNamingReadOnlyAccess

Description : fournit un accès en lecture seule à toutes les actions de dénomination automatique de Route 53.

AmazonRoute53AutoNamingReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRoute53AutoNamingReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 janvier 2018, 03:02 UTC
- Heure modifiée : 18 janvier 2018, 03:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRoute53AutoNamingRegistrantAccess

Description : Fournit un accès au niveau du titulaire aux actions de dénomination automatique de Route 53.

AmazonRoute53AutoNamingRegistrantAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRoute53AutoNamingRegistrantAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 mars 2018, 22:33 UTC
- Heure modifiée : 12 mars 2018, 22:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
    "*"
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRoute53DomainsFullAccess

Description : fournit un accès complet à toutes les actions de Route53 Domains et Create Hosted Zone pour permettre la création d'une zone hébergée dans le cadre des enregistrements de domaines.

AmazonRoute53DomainsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRoute53DomainsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 06 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRoute53DomainsReadOnlyAccess

Description : Permet d'accéder à la liste des domaines et aux actions de Route53.

AmazonRoute53DomainsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRoute53DomainsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 06 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
    ]  
  }  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRoute53FullAccess

Description : fournit un accès complet à toutes les fonctionnalités d'Amazon Route 53 via le Console de gestion AWS.

AmazonRoute53FullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRoute53FullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53FullAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRoute53GlobalResolverFullAccess

Description : fournit un accès complet pour récupérer, répertorier, créer, mettre à jour et supprimer toutes les ressources d'Amazon Route 53 Global Resolver.

AmazonRoute53GlobalResolverFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRoute53GlobalResolverFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 mars 2026, 20:27 UTC
- Heure modifiée : 09 mars 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53GlobalResolverFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRoute53GlobalResolverReadOnlyAccess

Description : fournit un accès en lecture seule pour récupérer et répertorier toutes les ressources d'Amazon Route 53 Global Resolver.

AmazonRoute53GlobalResolverReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRoute53GlobalResolverReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 mars 2026, 20:27 UTC
- Heure modifiée : 09 mars 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53GlobalResolverReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRoute53ProfilesFullAccess

Description : Cette politique accorde un accès complet aux ressources du profil Amazon Route 53.

AmazonRoute53ProfilesFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRoute53ProfilesFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 avril 2024, 18:30 UTC
- Heure modifiée : 27 août 2024, 19:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ProfilesFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRoute53ProfilesReadOnlyAccess

Description : Cette politique accorde un accès en lecture seule aux ressources du profil Amazon Route 53.

AmazonRoute53ProfilesReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRoute53ProfilesReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 avril 2024, 18:29 UTC
- Heure modifiée : 27 août 2024, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ProfilesReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
      "*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRoute53ReadOnlyAccess

Description : fournit un accès en lecture seule à l'ensemble d'Amazon Route 53 via le Console de gestion AWS.

AmazonRoute53ReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonRoute53ReadOnlyAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 15 novembre 2016, 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRoute53RecoveryClusterFullAccess

Description : fournit un accès complet à Amazon Route 53 Recovery Cluster

AmazonRoute53RecoveryClusterFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRoute53RecoveryClusterFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 août 2021, 18:37 UTC
- Heure modifiée : 18 août 2021, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "route53-recovery-cluster:*"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRoute53RecoveryClusterReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon Route 53 Recovery Cluster

AmazonRoute53RecoveryClusterReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRoute53RecoveryClusterReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 août 2021, 17:36 UTC
- Heure modifiée : 01 avril 2022, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:ListRoutingControls"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRoute53RecoveryControlConfigFullAccess

Description : fournit un accès complet à Amazon Route 53 Recovery Control Config

AmazonRoute53RecoveryControlConfigFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonRoute53RecoveryControlConfigFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 août 2021, 17:48 UTC
- Heure modifiée : 18 août 2021, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRoute53RecoveryControlConfigReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon Route 53 Recovery Control Config

AmazonRoute53RecoveryControlConfigReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRoute53RecoveryControlConfigReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 août 2021, 18:01 UTC
- Heure modifiée : 18 octobre 2023, 17:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRoute53RecoveryReadinessFullAccess

Description : fournit un accès complet à Amazon Route 53 Recovery Readiness

AmazonRoute53RecoveryReadinessFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRoute53RecoveryReadinessFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 18 août 2021, 16:45 UTC
- Heure modifiée : 18 août 2021, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRoute53RecoveryReadinessReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon Route 53 Recovery Readiness

AmazonRoute53RecoveryReadinessReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRoute53RecoveryReadinessReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 août 2021, 18:11 UTC
- Heure modifiée : 09 novembre 2021, 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:ListTagsForResource"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "route53-recovery-readiness:GetArchitectureRecommendations",
    "route53-recovery-readiness:GetCellReadinessSummary"
  ],
  "Resource" : "arn:aws:route53-recovery-readiness:*:*:*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRoute53ResolverFullAccess

Description : Politique d'accès complet pour Route 53 Resolver

AmazonRoute53ResolverFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRoute53ResolverFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 mai 2019, 18:10 UTC

- Heure modifiée : 05 août 2024, 20:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonRoute53ResolverReadOnlyAccess

Description : Politique en lecture seule pour Route 53 Resolver

AmazonRoute53ResolverReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonRoute53ResolverReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 mai 2019, 18:11 UTC
- Heure modifiée : 05 août 2024, 18:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ResolverReadOnlyAccess",
```

```
"Effect" : "Allow",
"Action" : [
    "route53resolver:Get*",
    "route53resolver:List*",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets"
],
"Resource" : [
    "*"
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonS3ExpressFullAccess

Description : fournit un accès complet à tous les compartiments de répertoires S3.

AmazonS3ExpressFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonS3ExpressFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 avril 2026, 20:42 UTC
- Heure modifiée : 03 avril 2026, 20:42 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonS3ExpressFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3ExpressFullAccess",
      "Effect" : "Allow",
      "Action" : "s3express:*",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonS3ExpressReadOnlyAccess

Description : fournit un accès en lecture seule aux opérations S3Express pour les compartiments de répertoires S3.

AmazonS3ExpressReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonS3ExpressReadOnlyAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 avril 2026, 20:42 UTC
- Heure modifiée : 03 avril 2026, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ExpressReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonS3FilesClientFullAccess

Description : permet au client root d'accéder à un système de fichiers S3 Files.

AmazonS3FilesClientFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonS3FilesClientFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 avril 2026, 12:57 UTC
- Heure modifiée : 07 avril 2026, 12:57 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3FilesClientFullAccess

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3FilesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3files:ClientMount",
        "s3files:ClientWrite",
        "s3files:ClientRootAccess"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonS3FilesClientReadOnlyAccess

Description : fournit un accès client en lecture seule à un système de fichiers S3 Files.

AmazonS3FilesClientReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonS3FilesClientReadOnlyAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 avril 2026, 12:57 UTC
- Heure modifiée : 07 avril 2026, 12:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FilesClientReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3FilesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3files:ClientMount"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonS3FilesClientReadWriteAccess

Description : fournit un accès client en lecture et en écriture à un système de fichiers S3 Files.

AmazonS3FilesClientReadWriteAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonS3FilesClientReadWriteAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 avril 2026, 12:57 UTC
- Heure modifiée : 07 avril 2026, 12:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FilesClientReadWriteAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3FilesPermissions",
```

```
    "Effect" : "Allow",
    "Action" : [
        "s3files:ClientMount",
        "s3files:ClientWrite"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonS3FilesCSIDriverPolicy

Description : fournit un accès de gestion aux ressources Amazon S3 Files

AmazonS3FilesCSIDriverPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonS3FilesCSIDriverPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 07 avril 2026, 13:12 UTC
- Heure modifiée : 07 avril 2026, 13:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3FilesCSIDriverPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonS3FilesFullAccess

Description : fournit un accès complet à tous les fichiers S3 via le Console de gestion AWS.

AmazonS3FilesFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonS3FilesFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 avril 2026, 12:42 UTC
- Heure modifiée : 07 avril 2026, 12:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FilesFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/D0-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"
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonS3FilesReadOnlyAccess

Description : fournit un accès en lecture seule à tous les fichiers S3 via le Console de gestion AWS.

AmazonS3FilesReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonS3FilesReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 avril 2026, 12:57 UTC
- Heure modifiée : 07 avril 2026, 12:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FilesReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonS3FullAccess

Description : Fournit un accès complet à tous les compartiments via le Console de gestion AWS.

AmazonS3FullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonS3FullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 27 septembre 2021, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:*",
        "s3-object-lambda:*"
      ],
    }
  ],
}
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonS3ObjectLambdaExecutionRolePolicy

Description : fournit aux fonctions AWS Lambda les autorisations nécessaires pour interagir avec Amazon S3 Object Lambda. Octroie également à Lambda les autorisations nécessaires pour écrire dans les CloudWatch journaux.

AmazonS3ObjectLambdaExecutionRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonS3ObjectLambdaExecutionRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 18 août 2021, 10:07 UTC
- Heure modifiée : 18 août 2021, 10:07 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonS3OutpostsFullAccess

Description : fournit un accès complet à Amazon S3 sur Outposts via le Console de gestion AWS.

AmazonS3OutpostsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonS3OutpostsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 octobre 2020, 17:26 UTC
- Heure modifiée : 02 octobre 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonS3OutpostsReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon S3 sur Outposts via le Console de gestion AWS.

AmazonS3OutpostsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonS3OutpostsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 octobre 2020, 18:55 UTC

- Heure modifiée : 02 octobre 2020, 18:55 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonS3ReadOnlyAccess

Description : Fournit un accès en lecture seule à tous les compartiments via le Console de gestion AWS.

AmazonS3ReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonS3ReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 10 août 2023, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonS3TablesFullAccess

Description : fournit un accès complet à tous les compartiments de tables S3.

AmazonS3TablesFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonS3TablesFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 décembre 2024, 15:21 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3TablesFullAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonS3TablesLakeFormationServiceRole

Description : Cette politique gérée accorde à AWS Lake Formation les autorisations nécessaires pour agir sur tous les compartiments de tables, espaces de noms et tables du compte.

AmazonS3TablesLakeFormationServiceRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonS3TablesLakeFormationServiceRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 19 juin 2025, 19:07 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonS3TablesLakeFormationServiceRole

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid" : "KMSSDataAccessPermissionsForS3TablesResources",
    "Effect" : "Allow",
    "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringLike" : {
            "kms:ViaService" : [
                "s3.*.amazonaws.com"
            ],
            "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3tables:*:*:bucket/*/table/*"
        },
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid" : "KMSSDescribeKeyAccessPermissionsForS3TablesResources",
    "Effect" : "Allow",
    "Action" : [
        "kms:DescribeKey"
    ],
    "Resource" : "*",
    "Condition" : {

```

```
    "StringLike" : {
      "kms:ViaService" : [
        "s3tables.*.amazonaws.com"
      ]
    },
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonS3TablesReadOnlyAccess

Description : fournit un accès en lecture seule à tous les compartiments de tables S3.

AmazonS3TablesReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonS3TablesReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 décembre 2024, 15:21 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3TablesReadOnlyAccess

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:Get*",
        "s3tables:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

Description : Politique de rôle de service utilisée par le service de Service AWS catalogue pour approvisionner des produits du SageMaker portefeuille de produits Amazon. Accorde des autorisations à un ensemble de services connexes CodePipeline CodeBuild, notamment CodeCommit,, CloudFormation, Glue, etc.

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 novembre 2020, 18:48 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "AmazonSageMakerServiceCatalogGlueClassifierPermission",
    "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"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerCanvasAIServiceAccess

Description : autorise Amazon SageMaker Canvas à utiliser les services d'IA pour prendre en charge les solutions d'IA prêtes à l'emploi. Cette politique ajoutera d'autres autorisations mutantes pour les services à mesure qu'Amazon SageMaker Canvas ajoutera du support.

AmazonSageMakerCanvasAIServiceAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerCanvasAIServiceAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 mars 2023, 22:36 UTC
- Heure modifiée : 29 novembre 2023, 14:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServiceAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Texttract",
      "Effect" : "Allow",
      "Action" : [
        "texttract:AnalyzeDocument",
        "texttract:AnalyzeExpense",
        "texttract:AnalyzeID",
        "texttract:StartDocumentAnalysis",
        "texttract:StartExpenseAnalysis",
        "texttract:GetDocumentAnalysis",
        "texttract: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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerCanvasBedrockAccess

Description : Cette politique autorise l'utilisation d'Amazon Bedrock dans SageMaker Canvas en donnant accès à des services en aval tels que S3.

AmazonSageMakerCanvasBedrockAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerCanvasBedrockAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 février 2024, 18:37 UTC
- Heure modifiée : 02 février 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
    ]
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerCanvasDataPrepFullAccess

Description : fournit un accès complet aux SageMaker ressources et opérations Amazon pour la préparation des données dans Canvas. La politique fournit également un accès sélectif aux services associés (par exemple, S3, IAM, KMS, RDS, CloudWatch Logs, Redshift, Athena, Glue EventBridge,

Secrets Manager). Cette politique doit être associée au rôle d'exécution d'Amazon SageMaker Domain/User Profile.

AmazonSageMakerCanvasDataPrepFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerCanvasDataPrepFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 octobre 2023, 22:56 UTC
- Heure modifiée : 16 août 2024, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerCanvasDirectDeployAccess

Description : permet à Amazon SageMaker Canvas de créer, de gérer et d'afficher les informations relatives aux terminaux créés via Canvas. Permet à Amazon SageMaker Canvas de récupérer les métriques d'invocation des terminaux à partir de CloudWatch.

AmazonSageMakerCanvasDirectDeployAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerCanvasDirectDeployAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 06 octobre 2023, 18:11 UTC
- Heure modifiée : 06 octobre 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy

Description : Cette politique accorde des autorisations à Amazon EMR Serverless pour des services tels que S3, utilisé par Amazon SageMaker Canvas pour le traitement de données volumineuses.

AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 juillet 2024, 00:35 UTC
- Heure modifiée : 27 juillet 2024, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
    }
}
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerCanvasForecastAccess

Description : Cette politique accorde les autorisations généralement nécessaires pour utiliser SageMaker Canvas avec Amazon Forecast.

AmazonSageMakerCanvasForecastAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerCanvasForecastAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 24 août 2022, 20:04 UTC
- Heure modifiée : 24 août 2022, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerCanvasFullAccess

Description : fournit un accès complet aux ressources et aux opérations d'Amazon SageMaker Canvas. La politique fournit également un accès sélectif aux services associés (par exemple, S3,

IAM, VPC, ECR, CloudWatch Logs, Redshift, Secrets Manager et Forecast). Cette politique doit être associée au rôle d'exécution d'Amazon SageMaker Domain/User Profile.

AmazonSageMakerCanvasFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerCanvasFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 septembre 2022, 00:44 UTC
- Heure modifiée : 16 août 2024, 04:35 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess`

Version de la politique

Version de la politique : v11 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerCanvasSMDDataScienceAssistantAccess

Description : autorise Amazon SageMaker Canvas à utiliser le service SageMaker Data Science Assistant. L'assistant Data Science utilise actuellement Amazon SageMaker et Amazon Q Developer pour traiter les demandes des utilisateurs.

AmazonSageMakerCanvasSMDDataScienceAssistantAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerCanvasSMDDataScienceAssistantAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 décembre 2024, 14:06 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasSMDDataScienceAssistantAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerCapacityReservationServiceRolePolicy

Description : Cette politique autorise Amazon SageMaker Capacity Reservations à publier des CloudWatch statistiques sur les comptes clients afin d'améliorer la visibilité de l'utilisation.

AmazonSageMakerCapacityReservationServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 08 avril 2026, 20:27 UTC
- Heure modifiée : 08 avril 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCapacityReservationServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudwatchPutMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "aws/sagemaker/CapacityReservations"
        }
      }
    }
  ]
}
```



```
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerClusterInstanceRolePolicy

Description : Cette politique accorde les autorisations généralement nécessaires pour utiliser Amazon SageMaker Cluster.

AmazonSageMakerClusterInstanceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerClusterInstanceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2023, 15:11 UTC
- Heure modifiée : 29 novembre 2023, 15:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerCoreServiceRolePolicy

Description : Politique gérée pour le rôle lié à un service pour Amazon SageMaker Core Services

AmazonSageMakerCoreServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 21 décembre 2020, 21:40 UTC
- Heure modifiée : 21 décembre 2020, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerEdgeDeviceFleetPolicy

Description : fournit les autorisations nécessaires à SageMaker Edge pour créer et gérer un parc d'appareils pour le client à l'aide de la connexion cloud par défaut.

AmazonSageMakerEdgeDeviceFleetPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerEdgeDeviceFleetPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service

- Heure de création : 08 décembre 2020, 16:17 UTC
- Heure modifiée : 08 décembre 2020, 16:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            ]
        }
    }
}

```

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerFeatureStoreAccess

Description : fournit les autorisations nécessaires pour activer la boutique hors ligne pour un groupe de SageMaker FeatureStore fonctionnalités Amazon.

AmazonSageMakerFeatureStoreAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerFeatureStoreAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2020, 16:24 UTC
- Heure modifiée : 05 décembre 2022, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerFullAccess

Description : fournit un accès complet à Amazon SageMaker via le SDK Console de gestion AWS et. Fournit également un accès sélectif à des services connexes (par exemple, S3, ECR, CloudWatch Logs).

AmazonSageMakerFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2017, 13:07 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFullAccess`

Version de la politique

Version de la politique : v29 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerGeospatialExecutionRole

Description : Cette politique donne accès aux services généralement nécessaires à l'utilisation de la technologie SageMaker géospatiale.

AmazonSageMakerGeospatialExecutionRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerGeospatialExecutionRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 30 novembre 2022, 10:08 UTC
- Heure modifiée : 10 mai 2023, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerGeospatialFullAccess

Description : Cette politique accorde des autorisations qui permettent un accès complet à Amazon SageMaker Geospatial via le SDK Console de gestion AWS et.

AmazonSageMakerGeospatialFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerGeospatialFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 30 novembre 2022, 10:06 UTC
- Heure modifiée : 30 novembre 2022, 10:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
          ]
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerGroundTruthExecution

Description : Permet d'accéder aux AWS services nécessaires à l'exécution de la tâche SageMaker GroundTruth d'étiquetage

AmazonSageMakerGroundTruthExecution est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonSageMakerGroundTruthExecution` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 juillet 2020, 19:30 UTC
- Heure modifiée : 29 avril 2022, 20:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
      ]
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerHyperPodGatedModelAccess

Description : Cette politique gérée par Amazon fournit les autorisations nécessaires pour accéder SageMaker HyperPod aux modèles sécurisés dans SageMaker Jumpstart. Il permet de créer des URL présignées pour le contenu du hub dans le hub SageMaker public.

AmazonSageMakerHyperPodGatedModelAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerHyperPodGatedModelAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 janvier 2026, 01:04 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodGatedModelAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerHyperPodInferenceAccess

Description : Cette politique fournit les privilèges administratifs nécessaires à la configuration de l'opérateur SageMaker HyperPod d'inférence. Il permet à l'opérateur d'inférence d'accéder aux ressources AWS réseau, à Amazon S3, Amazon ECR, Amazon, AWS Certificate Manager CloudWatch, ainsi qu'aux SageMaker ressources nécessaires pour déployer et gérer les charges de travail d'inférence sur les clusters HyperPod

AmazonSageMakerHyperPodInferenceAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerHyperPodInferenceAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 janvier 2026, 20:34 UTC
- Heure modifiée : 20 juillet 2026, 20:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodInferenceAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  }
}
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerHyperPodInferenceGatewayAccess

Description : Cette politique fournit les autorisations nécessaires pour configurer et exploiter la passerelle SageMaker HyperPod d'inférence. Il permet à la passerelle de gérer les AWS certificats du gestionnaire de certificats (ACM) pour la terminaison TLS lors du déploiement et de la diffusion de charges de travail d'inférence sur des clusters. HyperPod

AmazonSageMakerHyperPodInferenceGatewayAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerHyperPodInferenceGatewayAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 septembre 2026, 23:27 UTC

- Heure modifiée : 09 septembre 2026, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodInferenceGatewayAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerHyperPodObservabilityAdminAccess

Description : Cette politique fournit les privilèges administratifs nécessaires à la configuration de l'Amazon SageMaker HyperPod observabilité. Il permet d'accéder à Amazon Managed Prometheus, Amazon

Managed Grafana et EKS Addons. La politique inclut également un accès étendu aux API HTTP Grafana via ServiceAccountTokens tous les espaces de travail Amazon Managed Grafana de votre compte.

AmazonSageMakerHyperPodObservabilityAdminAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerHyperPodObservabilityAdminAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 10 juillet 2025, 14:37 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodObservabilityAdminAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "EKSAaddonAccess",
  "Effect" : "Allow",
  "Action" : [
    "eks:DeleteAddon",
    "eks:UpdateAddon",

```

```

    "eks:DescribeAddon"
  ],
  "Resource" : "arn:aws:eks:*:*:addon/*/amazon-sagemaker-hyperpod-observability/*"
},
{
  "Sid" : "EKSAAddonDescribeAccess",
  "Effect" : "Allow",
  "Action" : [
    "eks:DescribeAddonConfiguration",
    "eks:DescribeAddonVersions"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EKSAAddonPodIdentityAccess",
  "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" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerHyperPodServiceRolePolicy

Description : Cette politique accorde des autorisations à Amazon SageMaker HyperPod pour les AWS services connexes tels qu'Amazon EKS, Amazon, CloudWatch etc.

AmazonSageMakerHyperPodServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 06 septembre 2024, 17:04 UTC
- Heure modifiée : 06 septembre 2024, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerHyperPodServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
      }
    }
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerHyperPodTrainingOperatorAccess

Description : Cette politique fournit les autorisations administratives nécessaires pour configurer l'opérateur SageMaker HyperPod de formation. Il permet d'accéder aux modules complémentaires Amazon SageMaker HyperPod et EKS. La politique inclut des autorisations permettant de décrire les SageMaker HyperPod ressources de votre compte.

AmazonSageMakerHyperPodTrainingOperatorAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerHyperPodTrainingOperatorAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 août 2025, 17:04 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodTrainingOperatorAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
    "Sid" : "AllowDescribeClusterNodeOnHyperPodClusters",
    "Effect" : "Allow",
    "Action" : "sagemaker:DescribeClusterNode",
    "Resource" : "arn:aws:sagemaker:*:*:cluster/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/SageMaker" : "true"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerInferenceServiceRolePolicy

Description : Politique gérée pour le rôle lié au service pour Amazon SageMaker Inference.

AmazonSageMakerInferenceServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 30 juillet 2026, 19:42 UTC
- Heure modifiée : 17 août 2026, 21:07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerInferenceServiceRolePolicy

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
    }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerJobFullAccess

Description : autorise les rôles SageMaker d'exécution des tâches Amazon à accéder aux données dans Amazon S3, à appeler des agents via Amazon Bedrock, à suivre des expériences avec MLflow AgentCore, à publier des packages de modèles, à écrire des journaux sur Amazon CloudWatch, à invoquer des fonctions AWS Lambda et à gérer les interfaces réseau Amazon VPC.

AmazonSageMakerJobFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerJobFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 juin 2026, 02:42 UTC
- Heure modifiée : 03 juin 2026, 02:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerJobFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "KMSSDescribeKey",
    "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}"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerJobRuntimeAccess

Description : autorise les environnements d'exécution des agents à invoquer les API d'exécution des SageMaker tâches Amazon utilisées lors de la personnalisation du modèle pour la génération d'échantillons, la réalisation de trajectoires et la soumission des récompenses.

AmazonSageMakerJobRuntimeAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerJobRuntimeAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 juin 2026, 02:42 UTC

- Heure modifiée : 07 août 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerJobRuntimeAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerMechanicalTurkAccess

Description : Permet de créer des FlowDefinition ressources Amazon Augmented AI pour n'importe quelle équipe de travail.

AmazonSageMakerMechanicalTurkAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonSageMakerMechanicalTurkAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 décembre 2019, 16:19 UTC
- Heure modifiée : 3 décembre 2019, 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerModelCustomizationCoreAccess

Description : accorde des autorisations pour les flux de travail de personnalisation des SageMaker modèles, y compris la formation sans serveur, la fonction de récompense personnalisée pour l'apprentissage par renforcement, l'évaluation des modèles et le déploiement sur des terminaux SageMaker ou Bedrock.

AmazonSageMakerModelCustomizationCoreAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerModelCustomizationCoreAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 mai 2026, 18:57 UTC
- Heure modifiée : 21 juillet 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelCustomizationCoreAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerModelGovernanceUseAccess

Description : Cette politique AWS gérée accorde les autorisations nécessaires pour utiliser toutes les fonctionnalités d'Amazon SageMaker Governance. La politique fournit également un accès sélectif aux services associés (par exemple, S3, KMS).

AmazonSageMakerModelGovernanceUseAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonSageMakerModelGovernanceUseAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 novembre 2022, 08:58 UTC
- Heure modifiée : 04 juin 2024, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerModelRegistryFullAccess

Description : Il s'agit d'une nouvelle politique gérée pour le registre des modèles dans Sagemaker. Cette politique est une politique autonome qui peut être associée au rôle utilisateur pour accéder aux fonctionnalités liées au Model Registry dans Sagemaker.

AmazonSageMakerModelRegistryFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerModelRegistryFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 avril 2023, 05:20 UTC

- Heure modifiée : 06 juin 2024, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerNotebooksServiceRolePolicy

Description : Politique gérée pour le rôle lié à un service pour Amazon SageMaker Notebooks

AmazonSageMakerNotebooksServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 18 octobre 2019, 20:27 UTC
- Heure modifiée : 16 avril 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerPartnerAppsFullAccess

Description : permet aux utilisateurs des applications SageMaker partenaires Amazon d'accéder aux applications, de répertorier les applications disponibles, de lancer les interfaces utilisateur Web des applications et de se connecter via le SDK de l'application.

AmazonSageMakerPartnerAppsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerPartnerAppsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 janvier 2025, 18:37 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPartnerAppsFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy

Description : Politique de rôle de service utilisée par l' AWS APIGateway dans le cadre des produits fournis à AWS ServiceCatalog partir du portefeuille de produits Amazon SageMaker . Accorde des autorisations à un ensemble de services connexes, notamment Lambda et d'autres.

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 01 août 2023, 15:06 UTC
- Heure modifiée : 01 août 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy

Description : Politique de rôle de service utilisée AWS CloudFormation par les AWS ServiceCatalog produits fournis du SageMaker portefeuille de produits Amazon. Octroie des autorisations à un sous-ensemble de services connexes, notamment Lambda, APIGateway et d'autres.

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 01 août 2023, 15:06 UTC

- Heure modifiée : 01 août 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy

Description : Politique de rôle de service utilisée par le AWS Lambda dans le cadre des produits AWS ServiceCatalog provisionnés du SageMaker portefeuille de produits Amazon. Octroie des autorisations à un ensemble de services connexes, notamment Secrets Manager.

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 01 août 2023, 15:05 UTC
- Heure modifiée : 01 août 2023, 15:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerPipelinesIntegrations

Description : Cette politique gérée par Amazon accorde les autorisations généralement nécessaires pour une utilisation avec les étapes de rappel et les étapes Lambda dans SageMaker Model Building Pipelines. Il s'ajoute à AmazonSageMaker-ExecutionRole ce qui peut être créé lors de la configuration de SageMaker Studio. Il peut également être associé à tout autre rôle qui sera utilisé pour créer ou exécuter des pipelines.

AmazonSageMakerPipelinesIntegration est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerPipelinesIntegrations à vos utilisateurs, groupes et rôles.

Détails de la politique

- **Type** : politique AWS gérée
- **Heure de création** : 30 juillet 2021, 16:35 UTC

- Heure modifiée : 17 février 2023, 21:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPipelinesIntegrations`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
  }
}

```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerQuickSightVPCPolicy

Description : Cette politique sera utilisée par SageMaker Unified Studios pour créer des ressources liées au VPC pour QuickSight

AmazonSageMakerQuickSightVPCPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerQuickSightVPCPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 03 juin 2025, 17:37 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerQuickSightVPCPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageQuickSightVPCCConnection",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateVPCCConnection",
        "quicksight:DescribeVPCCConnection",
        "quicksight>DeleteVPCCConnection",
        "quicksight:ListVPCCConnections",
        "quicksight:UpdateVPCCConnection"
      ],
      "Resource" : "arn:aws:quicksight:*:*:vpccconnection/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeQuickSightVPCCConnectionEC2Resources",
      "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}"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerReadOnly

Description : fournit un accès en lecture seule à Amazon SageMaker via le SDK Console de gestion AWS et.

AmazonSageMakerReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2017, 13:07 UTC
- Heure modifiée : 01 décembre 2021, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerReadOnly`

Version de la politique

Version de la politique : v11 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy

Description : Politique de rôle de service utilisée par l' AWS APIGateway dans le cadre des produits fournis à AWS ServiceCatalog partir du portefeuille de produits Amazon SageMaker . Accorde des autorisations à un ensemble de services connexes, notamment CloudWatch Logs et autres.

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicyest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 25 mars 2022, 04:25 UTC
- Heure modifiée : 25 mars 2022, 04:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy

Description : Politique de rôle de service utilisée AWS CloudFormation par les AWS ServiceCatalog produits fournis du SageMaker portefeuille de produits Amazon. Octroie des autorisations à un sous-ensemble de services connexes, notamment SageMaker .

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service

- Heure de création : 25 mars 2022, 04:26 UTC
- Heure modifiée : 25 mars 2022, 04:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  ]
}

```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

Description : Politique de rôle de service utilisée AWS CodeBuild par les AWS ServiceCatalog produits fournis du SageMaker portefeuille de produits Amazon. Octroie des autorisations à un sous-ensemble de services connexes CodePipeline, CodeBuild notamment.

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 mars 2022, 04:27 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "AmazonSageMakerCodeBuildPassRolePermission",
    "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"
    }
}
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

Description : Politique de rôle de service utilisée AWS CodePipeline par les AWS ServiceCatalog produits fournis du SageMaker portefeuille de produits Amazon. Octroie des autorisations à un sous-ensemble de services connexes CodePipeline, CodeBuild notamment.

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 22 février 2022, 09:53 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

Description : Politique de rôle de service utilisée par les AWS CloudWatch événements dans le cadre des produits AWS ServiceCatalog provisionnés du SageMaker portefeuille de produits Amazon. Accorde des autorisations à un sous-ensemble de services connexes, y compris CodePipeline et d'autres.

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 22 février 2022, 09:53 UTC
- Heure modifiée : 22 février 2022, 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

Description : Politique de rôle de service utilisée par AWS Firehose dans le cadre des produits AWS ServiceCatalog fournis à partir du SageMaker portefeuille de produits Amazon. Accorde des autorisations à un ensemble de services connexes, notamment Firehose et d'autres.

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 22 février 2022, 09:54 UTC
- Heure modifiée : 22 février 2022, 09:54 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

Description : Politique de rôle de service utilisée par AWS Glue dans le cadre des AWS ServiceCatalog produits fournis à partir du SageMaker portefeuille de produits Amazon. Octroie des autorisations à un ensemble de services connexes, notamment Glue, S3 et autres.

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 22 février 2022, 09:51 UTC
- Heure modifiée : 26 août 2022, 19:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

Description : Politique de rôle de service utilisée par le AWS Lambda dans le cadre des produits AWS ServiceCatalog provisionnés du SageMaker portefeuille de produits Amazon. Octroie des autorisations à un ensemble de services connexes, notamment ECR, S3 et autres.

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 04 avril 2022, 16:34 UTC
- Heure modifiée : 11 juin 2024, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerSpacesControllerPolicy

Description : octroie à Systems Manager les autorisations d'activation, de gestion des sessions et d'opérations clés KMS requises pour que le SageMaker module complémentaire Spaces permette un accès distant sécurisé à EKS SageMaker Spaces.

AmazonSageMakerSpacesControllerPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerSpacesControllerPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 novembre 2025, 04:34 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerSpacesControllerPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerSpacesRouterPolicy

Description : accorde à Systems KMS les autorisations d'opérations clés requises pour que le routeur SageMaker Spaces permette un accès distant sécurisé à EKS SageMaker Spaces.

AmazonSageMakerSpacesRouterPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerSpacesRouterPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 19 novembre 2025, 04:34 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerSpacesRouterPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
      }
    }
  ]
}
```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSageMakerTrainingPlanCreateAccess

Description : Cette politique gérée par Amazon fournit les autorisations nécessaires pour créer et gérer des plans de SageMaker formation. Il permet aux utilisateurs de créer des plans de formation et des capacités réservées, de décrire les plans de formation existants et d'effectuer des opérations de recherche et de liste.

AmazonSageMakerTrainingPlanCreateAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSageMakerTrainingPlanCreateAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 décembre 2024, 13:21 UTC
- Heure modifiée : 12 février 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerTrainingPlanCreateAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSecurityLakeAdministrator

Description : fournit un accès complet à Amazon Security Lake et aux services associés nécessaires à l'administration de Security Lake.

AmazonSecurityLakeAdministrator est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSecurityLakeAdministrator à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 mai 2023, 22:04 UTC
- Heure modifiée : 23 février 2024, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "AllowRolePolicyActionsforSubscribersandSources",
    "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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSecurityLakeMetastoreManager

Description : Politique pour le gestionnaire de SecurityLake méta-magasins Amazon Lambda qui autorise l'accès à Cloudwatch, S3, Glue et SQS.

AmazonSecurityLakeMetastoreManager est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonSecurityLakeMetastoreManager` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 23 janvier 2024, 15:26 UTC
- Heure modifiée : 01 avril 2024, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSecurityLakePermissionsBoundary

Description : Amazon Security Lake crée des rôles IAM pour permettre à des sources personnalisées tierces d'écrire des données dans un lac de données et à des abonnés tiers de consommer des données provenant d'un lac de données. Il utilise cette politique lors de la création de ces rôles afin de définir la limite de leurs autorisations.

AmazonSecurityLakePermissionsBoundary est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSecurityLakePermissionsBoundary à vos utilisateurs, groupes et rôles.

Détails de la politique

- **Type** : politique AWS gérée
- **Heure de création** : 29 novembre 2022, 14:11 UTC
- **Heure modifiée** : 14 mai 2024, 20:39 UTC
- **ARN**: arn:aws:iam::aws:policy/AmazonSecurityLakePermissionsBoundary

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSESFullAccess

Description : fournit un accès complet à Amazon SES via le Console de gestion AWS.

AmazonSESFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSESFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 06 février 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSESReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon SES via le Console de gestion AWS.

AmazonSESReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSESReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 14 mai 2024, 12:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SESReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ses:Get*",
        "ses:List*",
        "ses:BatchGetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSESServiceRolePolicy

Description : Permet à SES de publier des mesures CloudWatch de surveillance de base d'Amazon pour le compte de vos ressources SES

AmazonSESServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 21 mai 2024, 16:02 UTC
- Heure modifiée : 21 mai 2024, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSESServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
          ]
        }
      }
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSNSFullAccess

Description : fournit un accès complet à Amazon SNS via le Console de gestion AWS.

AmazonSNSFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSNSFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 24 septembre 2024, 22:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSNSReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon SNS via le Console de gestion AWS.

AmazonSNSReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSNSReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 24 septembre 2024, 22:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

Rôle Amazon SNS

Description : Politique par défaut pour le rôle de service Amazon SNS.

AmazonSNSRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSNSRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 06 février 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSNSRole`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSQSFullAccess

Description : fournit un accès complet à Amazon SQS via le Console de gestion AWS.

AmazonSQSFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSQSFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 06 février 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
    "Effect" : "Allow",  
    "Resource" : "*"    
  }  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSQSReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon SQS via le Console de gestion AWS.

AmazonSQSReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSQSReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 24 mai 2024, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSQSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListMessageMoveTasks",
        "sqs:ListQueueTags"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSSMAutomationApproverAccess

Description : Permet de visualiser les exécutions d'automatisation et d'envoyer les décisions d'approbation à l'automatisation en attente d'approbation

AmazonSSMAutomationApproverAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSSMAutomationApproverAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 août 2017, 23:07 UTC
- Heure modifiée : 07 août 2017, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSSMAutomationRole

Description : Fournit des autorisations permettant au service d'automatisation EC2 d'exécuter les activités définies dans les documents d'automatisation

AmazonSSMAutomationRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSSMAutomationRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 05 décembre 2016, 22:09 UTC
- Heure modifiée : 20 mars 2026, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSSMDirectoryServiceAccess

Description : Cette politique permet à l'agent SSM d'accéder au service d'annuaire au nom du client pour rejoindre le domaine de l'instance gérée.

AmazonSSMDirectoryServiceAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSSMDirectoryServiceAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 mars 2019, 17:44 UTC

- Heure modifiée : 15 mars 2019, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSSMFullAccess

Description : fournit un accès complet à Amazon SSM.

AmazonSSMFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSSMFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 mai 2015, 17:39 UTC
- Heure modifiée : 20 novembre 2019, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSSMMaintenanceWindowRole

Description : Rôle de service à utiliser pour la fenêtre de maintenance EC2

AmazonSSMMaintenanceWindowRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSSMMaintenanceWindowRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 01 décembre 2016, 15:57 UTC
- Heure modifiée : 27 juillet 2019, 00:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:ListGroup",
        "resource-groups:ListGroupResources"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "tag:GetResources"
    ],
    "Resource" : [
        "*"
    ]
}
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSSMManagedEC2InstanceDefaultPolicy

Description : Cette politique active la fonctionnalité AWS Systems Manager sur les instances EC2.

AmazonSSMManagedEC2InstanceDefaultPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSSMManagedEC2InstanceDefaultPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 août 2022, 20:54 UTC
- Heure modifiée : 16 juillet 2024, 18:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSSMManagedInstanceCore

Description : Politique relative au rôle Amazon EC2 visant à activer les fonctionnalités principales du service AWS Systems Manager.

AmazonSSMManagedInstanceCore est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSSMManagedInstanceCore à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 mars 2019, 17:22 UTC
- Heure modifiée : 23 mai 2019, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSSMPatchAssociation

Description : Fournissez l'accès aux instances enfants pour l'opération d'association de correctifs.

AmazonSSMPatchAssociation est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSSMPatchAssociation à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 mai 2020, 16:00 UTC
- Heure modifiée : 13 mai 2020, 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMPatchAssociation`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSSMReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon SSM.

AmazonSSMReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSSMReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 mai 2015, 17:44 UTC
- Heure modifiée : 29 mai 2015, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSSMServiceRolePolicy

Description : Permet d'accéder aux AWS ressources gérées ou utilisées par Amazon SSM

AmazonSSMServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 13 novembre 2017, 19:20 UTC
- Heure modifiée : 26 juin 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy`

Version de la politique

Version de la politique : v17 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:ListGroup",
  "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*"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonSumerianFullAccess

Description : fournit un accès complet à Amazon Sumerian.

AmazonSumerianFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonSumerianFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 avril 2018, 20:14 UTC
- Heure modifiée : 24 avril 2018, 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSumerianFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonTextractFullAccess

Description : Accès à toutes les API Amazon Textract

AmazonTextractFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonTextractFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2018, 19:07 UTC
- Heure modifiée : 28 novembre 2018, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTextractFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonTextractServiceRole

Description : Permet à Textract d'appeler AWS les services en votre nom.

AmazonTextractServiceRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonTextractServiceRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 28 novembre 2018, 19:12 UTC
- Heure modifiée : 28 novembre 2018, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonTextractServiceRole`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "sns:Publish"
  ],
  "Resource" : "arn:aws:sns:*:*:AmazonTexttract*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonTimestreamConsoleFullAccess

Description : fournit un accès complet pour gérer Amazon Timestream à l'aide du. Console de gestion AWS Notez que cette politique accorde également des autorisations pour certaines opérations KMS et des opérations permettant de gérer vos requêtes enregistrées. Si vous utilisez la CMK gérée par le client, veuillez vous reporter à la documentation pour connaître les autorisations supplémentaires nécessaires.

AmazonTimestreamConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonTimestreamConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 septembre 2020, 21:47 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess

Version de la politique

Version de la politique : v13 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonTimestreamFullAccess

Description : fournit un accès complet à Amazon Timestream. Notez que cette politique accorde également l'accès à certaines opérations KMS. Si vous utilisez la CMK gérée par le client, veuillez vous reporter à la documentation pour connaître les autorisations supplémentaires nécessaires.

AmazonTimestreamFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonTimestreamFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 septembre 2020, 21:47 UTC
- Heure modifiée : 26 novembre 2021, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonTimestreamInfluxDBFullAccess

Description : fournit un accès administratif complet pour créer, mettre à jour, supprimer et répertorier les instances Amazon Timestream InfluxDB et créer et répertorier des groupes de paramètres. Reportez-vous à la documentation pour connaître les autorisations supplémentaires nécessaires.

AmazonTimestreamInfluxDBFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonTimestreamInfluxDBFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 mars 2024, 22:53 UTC
- Heure modifiée : 03 août 2026, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess`

Version de la politique

Version de la politique : v18 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-xcc5llpq4v1bc",
            "prod-rjppt7huo35fm"
          ]
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess

Description : fournit un accès administratif pour gérer les instances et les groupes de paramètres Amazon Timestream InfluxDB, à l'exception des opérations de la place de marché.

AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 avril 2025, 17:52 UTC
- Heure modifiée : 03 août 2026, 22:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:::*"
  ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonTimestreamInfluxDBServiceRolePolicy

Description : fournit un accès administratif complet pour créer, mettre à jour, supprimer et répertorier les instances Amazon Timestream InfluxDB et créer et répertorier des groupes de paramètres.

Reportez-vous à la documentation pour connaître les autorisations supplémentaires nécessaires.

AmazonTimestreamInfluxDBServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 14 mars 2024, 18:53 UTC
- Heure modifiée : 20 juillet 2026, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
    }
  }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonTimestreamReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon Timestream. La politique fournit également l'autorisation d'annuler toute requête en cours d'exécution. Si vous utilisez la CMK gérée par le client, veuillez consulter la documentation pour connaître les autorisations supplémentaires nécessaires.

AmazonTimestreamReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonTimestreamReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 septembre 2020, 21:47 UTC
- Heure modifiée : 05 juin 2024, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonTranscribeFullAccess

Description : fournit un accès complet aux opérations d'Amazon Transcribe

AmazonTranscribeFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonTranscribeFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 avril 2018, 16:06 UTC

- Heure modifiée : 04 avril 2018, 16:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3::*transcribe*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonTranscribeReadOnlyAccess

Description : Permet d'accéder au fonctionnement en lecture seule pour Amazon Transcribe

AmazonTranscribeReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonTranscribeReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 avril 2018, 16:05 UTC
- Heure modifiée : 04 avril 2018, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonVerifiedPermissionsFullAccess

Description : fournit un accès complet aux autorisations vérifiées

AmazonVerifiedPermissionsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonVerifiedPermissionsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 octobre 2024, 18:19 UTC
- Heure modifiée : 11 octobre 2024, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVerifiedPermissionsFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonVerifiedPermissionsReadOnlyAccess

Description : fournit un accès en lecture seule au service Verified Permissions.

AmazonVerifiedPermissionsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonVerifiedPermissionsReadOnlyAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 octobre 2024, 18:25 UTC
- Heure modifiée : 11 octobre 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVerifiedPermissionsReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonVPCCrossAccountNetworkInterfaceOperations

Description : Permet de créer des interfaces réseau et de les associer à des ressources multicomptes

AmazonVPCCrossAccountNetworkInterfaceOperation est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonVPCCrossAccountNetworkInterfaceOperations à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 juillet 2017, 20:47 UTC
- Heure modifiée : 25 septembre 2023, 15:12 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
    "*"
  ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonVPCFullAccess

Description : fournit un accès complet à Amazon VPC via le Console de gestion AWS.

AmazonVPCFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonVPCFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCFullAccess`

Version de la politique

Version de la politique : v13 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

Description : fournit les autorisations nécessaires pour décrire les AWS ressources, exécuter Network Access Analyzer et créer ou supprimer des balises dans Network Insights Access Scope et Network Insights Access Scope Analysis.

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonVPCNetworkAccessAnalyzerFullAccessPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 15 juin 2023, 22:56 UTC
- Heure modifiée : 14 août 2026, 17:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "TiroPermissions",
    "Effect" : "Allow",
    "Action" : [
        "tiros:CreateQuery",
        "tiros:GetQueryAnswer"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonVPCReachabilityAnalyzerFullAccessPolicy

Description : fournit les autorisations nécessaires pour décrire les AWS ressources, exécuter Reachability Analyzer et créer ou supprimer des balises sur Network Insights Path et Network Insights Analysis.

AmazonVPCReachabilityAnalyzerFullAccessPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonVPCReachabilityAnalyzerFullAccessPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 juin 2023, 20:12 UTC
- Heure modifiée : 14 août 2026, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerFullAccessPolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "TiroPermissions",
    "Effect" : "Allow",
    "Action" : [
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
    ],
    "Resource" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

Description : Cette politique est associée au rôle `IAMRoleForReachabilityAnalyzerCrossAccountResourceAccess`. Ce rôle est déployé sur les comptes membres d'une organisation lorsque le compte de gestion permet un accès sécurisé à Reachability Analyzer. Il fournit des autorisations pour consulter les ressources de l'ensemble de votre organisation à l'aide de la console Reachability Analyzer.

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonVPCReachabilityAnalyzerPathComponentReadPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 mai 2023, 20:38 UTC
- Heure modifiée : 01 mai 2023, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
"Effect" : "Allow",
"Action" : [
  "network-firewall:Describe*",
  "network-firewall:List*"
],
"Resource" : "*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonVPCReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon VPC via le Console de gestion AWS.

AmazonVPCReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonVPCReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonWorkDocsFullAccess

Description : Fournit un accès complet à Amazon WorkDocs via Console de gestion AWS

AmazonWorkDocsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonWorkDocsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 16 avril 2020, 23:05 UTC
- Heure modifiée : 16 avril 2020, 23:05 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonWorkDocsReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon WorkDocs via Console de gestion AWS

AmazonWorkDocsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonWorkDocsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 janvier 2020, 23:49 UTC
- Heure modifiée : 08 janvier 2020, 23:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonWorkMailEventsServiceRolePolicy

Description : Permet d'accéder à Amazon Events Services AWS et aux ressources utilisées ou gérées par Amazon WorkMail Events

AmazonWorkMailEventsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 16 avril 2019, 16:52 UTC
- Heure modifiée : 16 avril 2019, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonWorkMailFullAccess

Description : fournit un accès complet à Directory Service WorkMail, SES, EC2 et un accès en lecture aux métadonnées KMS.

AmazonWorkMailFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonWorkMailFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 21 décembre 2020, 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailFullAccess`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}

```



```
}  
  }  
    }  
      ]  
    }  
  }
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonWorkMailMessageFlowFullAccess

Description : Accès complet aux API WorkMail Message Flow

AmazonWorkMailMessageFlowFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonWorkMailMessageFlowFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 février 2021, 11:08 UTC
- Heure modifiée : 11 février 2021, 11:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonWorkMailMessageFlowReadOnlyAccess

Description : Accès en lecture seule aux WorkMail messages pour l' GetRawMessageContent API

AmazonWorkMailMessageFlowReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonWorkMailMessageFlowReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 janvier 2021, 12:40 UTC
- Heure modifiée : 28 janvier 2021, 12:40 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonWorkMailReadOnlyAccess

Description : fournit un accès en lecture seule à SES WorkMail et à SES.

AmazonWorkMailReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonWorkMailReadOnlyAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 25 juillet 2019, 08:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonWorkSpacesAdmin

Description : Permet d'accéder aux actions WorkSpaces administratives d'Amazon via le AWS SDK et l'interface de ligne de commande.

AmazonWorkSpacesAdmin est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonWorkSpacesAdmin à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 septembre 2015, 22:21 UTC
- Heure modifiée : 27 juin 2024, 17:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"    
  }  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonWorkSpacesApplicationManagerAdminAccess

Description : fournit un accès administrateur pour emballer une application dans Amazon WorkSpaces Application Manager.

AmazonWorkSpacesApplicationManagerAdminAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonWorkSpacesApplicationManagerAdminAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 avril 2015, 14:03 UTC
- Heure modifiée : 09 avril 2015, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesApplicationManagerAdminAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonWorkspacesPCAAccess

Description : Cette politique gérée fournit un accès administratif complet aux ressources de l'autorité de certification privée AWS Certificate Manager dans votre environnement Compte AWS pour l'authentification basée sur les certificats.

AmazonWorkspacesPCAAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonWorkspacesPCAAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 08 novembre 2022, 00:25 UTC
- Heure modifiée : 08 novembre 2022, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonWorkSpacesPoolServiceAccess

Description : Cette politique fournit un accès au AWS WorkSpaces service aux ressources du compte client requises pour le lancement de Workspaces Pools

AmazonWorkSpacesPoolServiceAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonWorkSpacesPoolServiceAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 juin 2024, 16:21 UTC
- Heure modifiée : 27 juin 2024, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesPoolServiceAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonWorkSpacesSecureBrowserReadOnly

Description : fournit un accès en lecture seule à Amazon WorkSpaces Secure Browser et à ses dépendances via le SDK et l'interface de ligne de commande AWS.

AmazonWorkSpacesSecureBrowserReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonWorkSpacesSecureBrowserReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 juin 2024, 20:01 UTC
- Heure modifiée : 24 juin 2024, 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSecureBrowserReadOnly`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonWorkSpacesSelfServiceAccess

Description : Permet d'accéder au service WorkSpaces backend Amazon pour effectuer des actions Workspace Self Service

AmazonWorkSpacesSelfServiceAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonWorkSpacesSelfServiceAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 juin 2019, 19:22 UTC
- Heure modifiée : 27 juin 2019, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonWorkSpacesServiceAccess

Description : permet d'accéder au AWS WorkSpaces service de lancement d'un espace de travail via le compte client.

AmazonWorkSpacesServiceAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonWorkSpacesServiceAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 juin 2019, 19:19 UTC
- Heure modifiée : 18 mars 2020, 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonWorkSpacesThinClientFullAccess

Description : fournit un accès complet à Amazon WorkSpaces Thin Client ainsi qu'un accès limité aux services connexes requis

AmazonWorkSpacesThinClientFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AmazonWorkSpacesThinClientFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 août 2024, 07:25 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesThinClientFullAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonWorkSpacesThinClientMonitoringServiceRolePolicy

Description : Permet d'accéder à Amazon Thin Client Monitoring Services AWS et aux ressources utilisées ou gérées par Amazon WorkSpaces Thin Client Monitoring

AmazonWorkSpacesThinClientMonitoringServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 13 juin 2025, 19:37 UTC
- Heure modifiée : 13 juin 2025, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesThinClientMonitoringServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
    "cloudwatch:PutMetricData"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : [
        "AWS/WorkSpacesThinClient",
        "AWS/Usage"
      ]
    }
  }
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonWorkSpacesThinClientReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon WorkSpaces Thin Client et à ses dépendances

AmazonWorkSpacesThinClientReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonWorkSpacesThinClientReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 juillet 2024, 08:50 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesThinClientReadOnlyAccess

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonWorkSpacesWebReadOnly

Description : fournit un accès en lecture seule à Amazon WorkSpaces Web et à ses dépendances via le SDK et l'interface Console de gestion AWS de ligne de commande.

AmazonWorkSpacesWebReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonWorkSpacesWebReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 novembre 2021, 14:20 UTC

- Heure modifiée : 02 novembre 2022, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonWorkSpacesWebServiceRolePolicy

Description : Permet d'accéder à Amazon Web Services AWS et aux ressources utilisées ou gérées par Amazon WorkSpaces Web

AmazonWorkSpacesWebServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 30 novembre 2021, 13:15 UTC
- Heure modifiée : 15 décembre 2022, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
    }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonZocaloFullAccess

Description : fournit un accès complet à Amazon Zocalo.

AmazonZocaloFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonZocaloFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 06 février 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmazonZocaloReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon Zocalo

AmazonZocaloReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmazonZocaloReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 06 février 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```

```
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AmplifyBackendDeployFullAccess

Description : fournit des autorisations d'accès complètes à Amplify pour déployer les ressources du backend Amplify (AWS AppSync, Amazon Cognito, Amazon S3 et autres services associés) via le kit de AWS Cloud développement (CDK)AWS

AmplifyBackendDeployFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AmplifyBackendDeployFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 06 octobre 2023, 21:32 UTC
- Heure modifiée : 14 novembre 2024, 19:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
      }
    }
  }
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AnthropicFullAccess

Description : Fournit un accès complet à la plateforme Claude sur AWS

AnthropicFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AnthropicFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 avril 2026, 04:57 UTC
- Heure modifiée : 25 septembre 2026, 20:17 UTC
- ARN: arn:aws:iam::aws:policy/AnthropicFullAccess

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AnthropicLimitedAccess

Description : Fournit un accès limité à la plateforme Claude sur AWS

AnthropicLimitedAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AnthropicLimitedAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 avril 2026, 04:57 UTC
- Heure modifiée : 02 octobre 2026, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AnthropicLimitedAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AnthropicReadOnlyAccess

Description : fournit un accès en lecture seule à la plateforme Claude sur AWS

AnthropicReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AnthropicReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 avril 2026, 04:57 UTC
- Heure modifiée : 02 octobre 2026, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AnthropicReadOnlyAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AnthropicSelfHostedEnvironmentAccess

Description : Permet de gérer un environnement auto-hébergé pour Claude Managed Agents

AnthropicSelfHostedEnvironmentAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AnthropicSelfHostedEnvironmentAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 juin 2026, 17:12 UTC
- Heure modifiée : 12 juin 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AnthropicSelfHostedEnvironmentAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

APIGatewayServiceRolePolicy

Description : permet à API Gateway de gérer les AWS ressources associées pour le compte du client.

APIGatewayServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 20 octobre 2017, 17:23 UTC
- Heure modifiée : 12 juillet 2021, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"  
    }  
  ]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AppIntegrationsServiceLinkedRolePolicy

Description : Permet AppIntegrations de gérer les AppFlow ressources et de publier des données CloudWatch métriques en votre nom.

AppIntegrationsServiceLinkedRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 30 septembre 2022, 19:42 UTC
- Heure modifiée : 30 septembre 2022, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ApplicationAutoScalingForAmazonAppStreamAccess

Description : Politique visant à activer la mise à l'échelle automatique des applications pour Amazon AppStream

ApplicationAutoScalingForAmazonAppStreamAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `ApplicationAutoScalingForAmazonAppStreamAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 06 février 2017, 21:39 UTC
- Heure modifiée : 06 février 2017, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ApplicationAutoScalingForAmazonAppStreamAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
    "cloudwatch:DescribeAlarms"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

Description : Permet d'accéder à la fonction d'exportation continue de l'Application Discovery Service Services AWS et aux ressources utilisées ou gérées par cette fonction

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 09 août 2018, 20:22 UTC
- Heure modifiée : 13 août 2018, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
}

```

```
}  
]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AppRunnerNetworkingServiceRolePolicy

Description : permet à AWS AppRunner Networking de gérer les AWS ressources associées en votre nom.

AppRunnerNetworkingServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 12 janvier 2022, 21:02 UTC
- Heure modifiée : 12 janvier 2022, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AppRunnerServiceRolePolicy

Description : Permet AWS AppRunner de gérer les AWS ressources associées en votre nom.

AppRunnerServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 14 mai 2021, 19:15 UTC
- Heure modifiée : 14 mai 2021, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
    }
  ]
}
```

```
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AppStudioServiceRolePolicy

Description : Permet AppStudio de gérer les AWS ressources associées en votre nom.

AppStudioServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 10 juillet 2024, 05:01 UTC
- Heure modifiée : 13 mars 2025, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppStudioServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
    }
}
}

```

```
]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AssuranceServiceRolePolicy

Description : Permet à AWS Assurance d'accéder à vos ressources pour les évaluations de conformité et la collecte de preuves.

AssuranceServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 26 août 2026, 21:07 UTC
- Heure modifiée : 26 août 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AssuranceServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
}
]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AuroraDsqlServiceLinkedRolePolicy

Description : Politique relative au rôle lié au service Amazon Aurora DSQL

AuroraDsqlServiceLinkedRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 03 décembre 2024, 15:06 UTC

- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AuroraDsqlServiceLinkedRolePolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/AuroraDSQL",
            "AWS/Usage"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AutoScalingConsoleFullAccess

Description : Fournit un accès complet à Auto Scaling via le Console de gestion AWS.

AutoScalingConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AutoScalingConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 janvier 2017, 19:43 UTC
- Heure modifiée : 06 février 2018, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AutoScalingConsoleReadOnlyAccess

Description : fournit un accès en lecture seule à Auto Scaling via le. Console de gestion AWS

AutoScalingConsoleReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AutoScalingConsoleReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 janvier 2017, 19:48 UTC
- Heure modifiée : 12 janvier 2017, 19:48 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AutoScalingFullAccess

Description : fournit un accès complet à Auto Scaling.

AutoScalingFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AutoScalingFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 janvier 2017, 19:31 UTC
- Heure modifiée : 06 février 2018, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AutoScalingNotificationAccessRole

Description : stratégie par défaut pour le rôle de service d'accès aux AutoScaling notifications.

AutoScalingNotificationAccessRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AutoScalingNotificationAccessRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 06 février 2015, 18:41 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AutoScalingNotificationAccessRole`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AutoScalingReadOnlyAccess

Description : fournit un accès en lecture seule à Auto Scaling.

AutoScalingReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AutoScalingReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 janvier 2017, 19:39 UTC
- Heure modifiée : 12 janvier 2017, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AutoScalingServiceRolePolicy

Description : Permet d'accéder aux ressources utilisées ou gérées par Auto Scaling Services AWS et de les utiliser

AutoScalingServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 08 janvier 2018, 23:10 UTC
- Heure modifiée : 12 novembre 2025, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWS-SSM-Automation-DiagnosisBucketPolicy

Description : fournit les autorisations nécessaires pour accéder au compartiment SSM Diagnosis S3 à des fins de diagnostic et de résolution des problèmes.

AWS-SSM-Automation-DiagnosisBucketPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWS-SSM-Automation-DiagnosisBucketPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 novembre 2024, 23:31 UTC
- Heure modifiée : 15 novembre 2024, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-Automation-DiagnosisBucketPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy

Description : autorisez le diagnostic des problèmes liés aux services SSM en exécutant les activités définies dans Automation Documents, principalement utilisées pour exécuter les documents Automation dans une configuration inter-comptes inter-régions en déclenchant des automatisations secondaires dans les comptes membres.

AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 16 novembre 2024, 00:01 UTC
- Heure modifiée : 29 août 2026, 00:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy

Description : autorisez le diagnostic des problèmes liés aux services SSM en exécutant les activités définies dans Automation Documents, principalement utilisées pour exécuter les documents Automation dans une account/region configuration cible en diagnostiquant l'état du service SSM sur tous les nœuds.

AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 16 novembre 2024, 00:08 UTC
- Heure modifiée : 28 août 2026, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy

Description : Fournit des autorisations aux comptes opérationnels afin de diagnostiquer les nœuds non gérés en fournissant les autorisations spécifiques à l'organisation requises par l'automatisation SSM pour extraire la liste des comptes membres à la racine d'une organisation afin de déclencher une exécution inter-comptes entre régions en permettant d'assumer des rôles d'exécution dans la cible. account/region

AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 16 novembre 2024, 00:11 UTC
- Heure modifiée : 16 novembre 2024, 00:11 UTC
- ARN: arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWS-SSM-RemediationAutomation-AdministrationRolePolicy

Description : Autorisez la résolution des problèmes liés aux services SSM en exécutant les activités définies dans Automation Documents, principalement utilisées pour exécuter les documents Automation dans une configuration inter-comptes inter-régions en déclenchant des automatisations secondaires dans les comptes membres.

AWS-SSM-RemediationAutomation-AdministrationRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWS-SSM-RemediationAutomation-AdministrationRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 16 novembre 2024, 00:14 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-AdministrationRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWS-SSM-RemediationAutomation-ExecutionRolePolicy

Description : fournit des autorisations pour résoudre les problèmes liés aux services SSM en exécutant les activités définies dans Automation Documents, principalement utilisées pour exécuter les documents Automation dans une account/region configuration cible en corrigeant l'état de santé des services SSM sur tous les nœuds.

AWS-SSM-RemediationAutomation-ExecutionRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWS-SSM-RemediationAutomation-ExecutionRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 16 novembre 2024, 00:17 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-ExecutionRolePolicy

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy

Description : Fournit des autorisations aux comptes opérationnels pour corriger les nœuds non gérés en fournissant les autorisations spécifiques à l'organisation requises par l'automatisation SSM pour extraire la liste des comptes membres à la racine d'une organisation afin de déclencher une exécution intercomptes entre régions en permettant d'assumer des rôles d'exécution dans la cible. account/region

AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 16 novembre 2024, 00:25 UTC
- Heure modifiée : 16 novembre 2024, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
      }
    }
  ]
}
```

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWS_ ConfigRole

Description : stratégie par défaut pour le rôle de service AWS Config. Fournit les autorisations nécessaires pour que AWS Config puisse suivre les modifications apportées à vos AWS ressources.

AWS_ConfigRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWS_ConfigRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 15 septembre 2020, 20:30 UTC
- Heure modifiée : 23 septembre 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWS_ConfigRole`

Version de la politique

Version de la politique : v73 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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",
"finespace:GetEnvironment",
"finespace: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:ListGroupsWith",
"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:GetFirmwareTask",
"iotwireless:GetMulticastGroup",
"iotwireless:GetNetworkAnalyzerConfiguration",
"iotwireless:GetServiceProfile",
"iotwireless:GetWirelessDevice",
"iotwireless:GetWirelessDeviceImportTask",
"iotwireless:GetWirelessGateway",
"iotwireless:GetWirelessGatewayTaskDefinition",
"iotwireless:ListDestinations",
"iotwireless:ListDeviceProfiles",
"iotwireless:ListDevicesForWirelessDeviceImportTask",
"iotwireless:ListFirmwareTasks",
"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:DescribeVPCCConnection",
"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:DescribeSenderId",
"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/*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAccountActivityAccess

Description : permet aux utilisateurs d'accéder à la page d'activité du compte.

AWSAccountActivityAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSAccountActivityAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 20 février 2026, 20:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountActivityAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAccountManagementFullAccess

Description : fournit un accès complet à la gestion des AWS comptes.

AWSAccountManagementFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSAccountManagementFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 septembre 2021, 23:20 UTC
- Heure modifiée : 30 septembre 2021, 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAccountManagementReadOnlyAccess

Description : fournit un accès en lecture seule à la gestion des comptes AWS

AWSAccountManagementReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSAccountManagementReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 septembre 2021, 23:29 UTC
- Heure modifiée : 30 septembre 2021, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAccountSettingsManagementRole

Description : fournit les autorisations requises pour gérer un compte pour les AWS applications.

AWSAccountSettingsManagementRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSAccountSettingsManagementRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 décembre 2025, 17:49 UTC
- Heure modifiée : 30 septembre 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountSettingsManagementRole`

Version de la politique

Version de la politique : v11 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAccountUsageReportAccess

Description : permet aux utilisateurs d'accéder à la page du rapport d'utilisation du compte.

AWSAccountUsageReportAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSAccountUsageReportAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 06 février 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountUsageReportAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAgentlessDiscoveryService

Description : permet au Discovery Agentless Connector d'accéder à l'enregistrement auprès d' AWS Application Discovery Service.

AWSAgentlessDiscoveryService est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSAgentlessDiscoveryService à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 août 2016, 01:35 UTC
- Heure modifiée : 24 février 2020, 23:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAgentRegistryServiceRolePolicy

Description : Permet au registre des AWS agents d'accéder aux ressources de AWS service en votre nom

AWSAgentRegistryServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 06 août 2026, 14:27 UTC
- Heure modifiée : 21 août 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAgentRegistryServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  }
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAppConfigServiceRolePolicy

Description : Permet AWS AppConfig d'appeler AWS les services en votre nom.

AWSAppConfigServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 08 mai 2026, 18:42 UTC

- Heure modifiée : 08 mai 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppConfigServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAppFabricFullAccess

Description : fournit un accès complet au AWS AppFabric service et un accès en lecture seule aux services dépendants tels que S3, Kinesis, KMS.

AWSAppFabricFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSAppFabricFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 juin 2023, 19:51 UTC
- Heure modifiée : 27 juin 2023, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAppFabricReadOnlyAccess

Description : Fournit un accès en lecture seule au AWS AppFabric

AWSAppFabricReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSAppFabricReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 juin 2023, 19:52 UTC
- Heure modifiée : 27 juin 2023, 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAppFabricServiceRolePolicy

Description : Permet AppFabric d'accéder à AWS des ressources en votre nom

AWSAppFabricServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle

- Heure de création : 26 juin 2023, 21:07 UTC
- Heure modifiée : 26 juin 2023, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppFabricServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationAutoscalingAppStreamFleetPolicy

Description : Politique accordant des autorisations à Application Auto Scaling pour accéder à AppStream et CloudWatch.

AWSApplicationAutoscalingAppStreamFleetPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle

- Heure de création : 20 octobre 2017, 19:04 UTC
- Heure modifiée : 20 octobre 2017, 19:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationAutoscalingCassandraTablePolicy

Description : Politique accordant des autorisations à Application Auto Scaling pour accéder à Cassandra et CloudWatch.

AWSApplicationAutoscalingCassandraTablePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 18 mars 2020, 22:49 UTC
- Heure modifiée : 18 mars 2020, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationAutoscalingComprehendEndpointPolicy

Description : Politique accordant des autorisations à Application Auto Scaling pour accéder à Comprehend et CloudWatch.

AWSApplicationAutoscalingComprehendEndpointPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 14 novembre 2019, 18:39 UTC
- Heure modifiée : 14 novembre 2019, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingComprehendEndpointPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationAutoScalingCustomResourcePolicy

Description : Politique accordant des autorisations à Application Auto Scaling pour accéder à APIGateway et CloudWatch pour une mise à l'échelle personnalisée des ressources

AWSApplicationAutoScalingCustomResourcePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 04 juin 2018, 23:22 UTC
- Heure modifiée : 04 juin 2018, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationAutoscalingDynamoDBTablePolicy

Description : Politique accordant des autorisations à Application Auto Scaling pour accéder à DynamoDB et. CloudWatch

AWSApplicationAutoscalingDynamoDBTablePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 20 octobre 2017, 21:34 UTC
- Heure modifiée : 20 octobre 2017, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "dynamodb:DescribeTable",
      "dynamodb:UpdateTable",
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:DescribeAlarms",
      "cloudwatch:DeleteAlarms"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

Description : Politique accordant des autorisations à Application Auto Scaling pour accéder à EC2 Spot Fleet et CloudWatch.

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 25 octobre 2017, 18:23 UTC
- Heure modifiée : 25 octobre 2017, 18:23 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationAutoscalingECSServicePolicy

Description : Politique accordant des autorisations à Application Auto Scaling pour accéder à EC2 Container Service et CloudWatch.

AWSApplicationAutoscalingECSServicePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 25 octobre 2017, 23:53 UTC
- Heure modifiée : 20 mai 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
        "ecs:DescribeServiceRevisions",
        "ecs:UpdateService",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch>DeleteAlarms"
    ],
    "Resource" : [
        "*"
    ]
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationAutoscalingElastiCacheRGPolicy

Description : Politique accordant des autorisations à Application Auto Scaling pour accéder à Amazon ElastiCache et Amazon CloudWatch.

AWSApplicationAutoscalingElastiCacheRGPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 17 août 2021, 23:41 UTC
- Heure modifiée : 26 mars 2025, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingElastiCacheRGPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
    ]
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationAutoscalingEMRInstanceGroupPolicy

Description : Politique accordant des autorisations à Application Auto Scaling pour accéder à Elastic Map Reduce et CloudWatch.

AWSApplicationAutoscalingEMRInstanceGroupPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 26 octobre 2017, 00:57 UTC
- Heure modifiée : 26 octobre 2017, 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationAutoscalingKafkaClusterPolicy

Description : Politique accordant des autorisations à Application Auto Scaling pour accéder à Managed Streaming pour Apache Kafka et CloudWatch.

AWSApplicationAutoscalingKafkaClusterPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 24 août 2020, 18:36 UTC
- Heure modifiée : 24 août 2020, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationAutoscalingLambdaConcurrencyPolicy

Description : Politique accordant des autorisations à Application Auto Scaling pour accéder à Lambda et CloudWatch.

AWSApplicationAutoscalingLambdaConcurrencyPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 21 octobre 2019, 20:04 UTC
- Heure modifiée : 21 octobre 2019, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "lambda:PutProvisionedConcurrencyConfig",
      "lambda:GetProvisionedConcurrencyConfig",
      "lambda>DeleteProvisionedConcurrencyConfig",
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:DescribeAlarms",
      "cloudwatch>DeleteAlarms"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationAutoscalingNeptuneClusterPolicy

Description : Politique accordant des autorisations à Application Auto Scaling pour accéder à Amazon Neptune et Amazon CloudWatch.

AWSApplicationAutoscalingNeptuneClusterPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 02 septembre 2021, 21:14 UTC

- Heure modifiée : 02 septembre 2021, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingNeptuneClusterPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationAutoscalingRDSClusterPolicy

Description : Politique accordant des autorisations à Application Auto Scaling pour accéder à RDS et CloudWatch.

AWSApplicationAutoscalingRDSClusterPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 17 octobre 2017, 17:46 UTC
- Heure modifiée : 07 août 2018, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationAutoscalingSageMakerEndpointPolicy

Description : Politique accordant des autorisations à Application Auto Scaling pour accéder à SageMaker et CloudWatch.

AWSApplicationAutoscalingSageMakerEndpointPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 06 février 2018, 19:58 UTC
- Heure modifiée : 13 novembre 2023, 18:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
    ]
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationAutoscalingWorkSpacesPoolPolicy

Description : Politique accordant des autorisations à Application Auto Scaling pour accéder à Amazon WorkSpaces et Amazon CloudWatch.

AWSApplicationAutoscalingWorkSpacesPoolPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 17 juin 2024, 18:39 UTC
- Heure modifiée : 17 juin 2024, 18:39 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingWorkSpacesPoolPolicy

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
      }
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationDiscoveryAgentAccess

Description : permet à l'agent Discovery de s'enregistrer auprès AWS d'Application Discovery Service.

AWSApplicationDiscoveryAgentAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSApplicationDiscoveryAgentAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 11 mai 2016, 21:38 UTC
- Heure modifiée : 24 février 2020, 22:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationDiscoveryAgentlessCollectorAccess

Description : Permet aux collecteurs sans agent Application Discovery Service de se mettre à jour automatiquement, de s'enregistrer et de communiquer avec Application Discovery Service

AWSApplicationDiscoveryAgentlessCollectorAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSApplicationDiscoveryAgentlessCollectorAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 16 août 2022, 21:00 UTC
- Heure modifiée : 16 août 2022, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentlessCollectorAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationDiscoveryServiceFullAccess

Description : fournit un accès complet pour afficher et baliser les éléments de configuration gérés par l' AWS Application Discovery Service

AWSApplicationDiscoveryServiceFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSApplicationDiscoveryServiceFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 mai 2016, 21:30 UTC
- Heure modifiée : 19 juin 2019, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryServiceFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      ]
    }
  }
}
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationMigrationAgentInstallationPolicy

Description : Cette politique permet d'installer l'agent de AWS réplication, qui est utilisé avec le service de migration des AWS applications (MGN) pour migrer des serveurs externes vers. AWS Associez cette politique à vos utilisateurs ou rôles IAM dont vous fournissez les informations d'identification lors de l'installation de l'agent de AWS réplication.

AWSApplicationMigrationAgentInstallationPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSApplicationMigrationAgentInstallationPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 juin 2022, 07:51 UTC
- Heure modifiée : 20 septembre 2022, 11:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentInstallationPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationMigrationAgentPolicy

Description : Cette politique autorise l'installation et l'utilisation de l'agent de AWS réplication, qui est utilisé avec le service de migration des AWS applications (MGN) pour migrer des serveurs externes. AWS Associez cette politique à vos utilisateurs ou rôles IAM dont vous fournissez les informations d'identification lors de l'installation de l'agent de AWS réplication.

AWSApplicationMigrationAgentPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSApplicationMigrationAgentPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 avril 2021, 07:00 UTC
- Heure modifiée : 20 septembre 2022, 11:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationMigrationAgentPolicy_v2

Description : Cette politique permet d'utiliser l'agent de AWS réplication, qui est utilisé avec le service de migration des AWS applications (MGN) pour migrer des serveurs externes vers. AWS Nous vous déconseillons d'associer cette politique à vos utilisateurs ou rôles IAM.

AWSApplicationMigrationAgentPolicy_v2 est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSApplicationMigrationAgentPolicy_v2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 06 juin 2022, 14:14 UTC
- Heure modifiée : 06 juin 2022, 14:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationMigrationConversionServerPolicy

Description : Cette politique permet au serveur de conversion du service de migration des applications (MGN), qui sont des instances EC2 lancées par le service de migration des applications, de communiquer avec le service MGN. Un rôle IAM avec cette politique est attaché (en tant que profil d'instance EC2) par MGN aux serveurs de conversion MGN, qui sont automatiquement lancés et interrompus par MGN, en cas de besoin. Nous vous déconseillons d'associer cette politique à vos utilisateurs ou rôles IAM. Les serveurs de conversion MGN sont utilisés par le service de migration des applications lorsque les utilisateurs choisissent de lancer des instances de test ou de basculement à l'aide de la console, de l'interface de ligne de commande ou de l'API MGN.

AWSApplicationMigrationConversionServerPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSApplicationMigrationConversionServerPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 07 avril 2021, 06:48 UTC
- Heure modifiée : 07 avril 2021, 06:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationConversionServerPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationMigrationEC2Access

Description : Cette politique fournit les opérations Amazon EC2 requises pour utiliser Application Migration Service (MGN) afin de lancer les serveurs migrés en tant qu'instances EC2. Associez cette politique à vos utilisateurs ou rôles IAM.

AWSApplicationMigrationEC2Access est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSApplicationMigrationEC2Access à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 avril 2021, 07:05 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationMigrationFSxProxyPolicy

Description : Fournit les autorisations nécessaires pour gérer le système de fichiers ONTAP

AWSApplicationMigrationFSxProxyPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSApplicationMigrationFSxProxyPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 31 mai 2026, 13:12 UTC
- Heure modifiée : 09 août 2026, 12:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationFSxProxyPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationMigrationFSxProxyVPCPolicy

Description : Fournit des autorisations de gestion PrivateLink entre le service de migration des AWS applications et le système de fichiers FSx du client

AWSApplicationMigrationFSxProxyVPCPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSApplicationMigrationFSxProxyVPCPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 31 mai 2026, 13:27 UTC
- Heure modifiée : 31 mai 2026, 13:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationFSxProxyVPCPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            }
        }
    }
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationMigrationFullAccess

Description : cette politique fournit des autorisations à toutes les API publiques d' AWS Application Migration Service (MGN), ainsi que des autorisations pour lire les informations clés de KMS. Associez cette politique à vos utilisateurs ou rôles IAM.

AWSApplicationMigrationFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSApplicationMigrationFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 avril 2021, 06:56 UTC
- Heure modifiée : 03 août 2026, 10:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess`

Version de la politique

Version de la politique : v14 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  ]
}
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationMigrationMGHAccess

Description : Cette politique permet au Service de migration des AWS applications (MGN) d'envoyer des métadonnées sur la progression des serveurs en cours de migration à l'aide de MGN vers AWS Migration Hub (MGH). MGN crée automatiquement un rôle IAM associé à cette politique et assume ce rôle. Nous vous déconseillons d'associer cette politique à vos utilisateurs ou rôles IAM.

AWSApplicationMigrationMGHAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSApplicationMigrationMGHAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 07 avril 2021, 07:10 UTC
- Heure modifiée : 07 avril 2021, 07:10 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationMGHAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationMigrationNetworkMigrationCustomResource

Description : Fournit des autorisations pour la ressource personnalisée de migration réseau

AWSApplicationMigrationNetworkMigrationCustomResource est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSApplicationMigrationNetworkMigrationCustomResource à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 novembre 2025, 11:34 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationNetworkMigrationCustomResource`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationMigrationNetworkMigrationMultiAccount

Description : Fournit les autorisations nécessaires pour automatiser la migration de VMware vers l'infrastructure AWS réseau via CloudFormation

AWSApplicationMigrationNetworkMigrationMultiAccount est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSApplicationMigrationNetworkMigrationMultiAccount à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 10 novembre 2025, 09:04 UTC
- Heure modifiée : 15 septembre 2026, 13:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationNetworkMigrationMultiAccount`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:DescribeInstanceState",
    "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"
        }
    }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationMigrationReadOnlyAccess

Description : Cette politique fournit des autorisations à toutes les API publiques en lecture seule d'Application Migration Service (MGN), ainsi qu'à certaines API en lecture seule d'autres AWS services qui sont requises pour utiliser pleinement la console MGN en lecture seule. Associez cette politique à vos utilisateurs ou rôles IAM.

AWSApplicationMigrationReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSAApplicationMigrationReadOnlyAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 avril 2021, 07:15 UTC
- Heure modifiée : 01 juillet 2026, 14:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationMigrationReplicationServerPolicy

Description : Cette politique permet aux serveurs de réplication du service de migration des applications (MGN), qui sont des instances EC2 lancées par le service de migration des applications, de communiquer avec le service MGN et de créer des instantanés EBS dans votre. Compte AWS. Un rôle IAM avec cette politique est attaché (en tant que profil d'instance EC2) par le service de migration des applications aux serveurs de réplication MGN qui sont automatiquement lancés et fermés par MGN, selon les besoins. Les serveurs de réplication MGN sont utilisés pour faciliter la réplication des données depuis vos serveurs externes vers AWS, dans le cadre du processus de migration géré à l'aide de MGN. Nous vous déconseillons d'associer cette politique à vos utilisateurs ou rôles IAM.

AWSApplicationMigrationReplicationServerPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSApplicationMigrationReplicationServerPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 07 avril 2021, 07:21 UTC
- Heure modifiée : 31 mai 2026, 13:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationReplicationServerPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationMigrationServiceEc2InstancePolicy

Description : Cette politique permet d'installer et d'utiliser l'agent de AWS réplique, qui est utilisé par le service de migration des AWS applications (AWS MGN) pour migrer les serveurs sources qui s'exécutent sur EC2 (entre régions ou entre AZ). Un rôle IAM avec cette politique doit être attaché (en tant que profil d'instance EC2) aux instances EC2.

AWSApplicationMigrationServiceEc2InstancePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSApplicationMigrationServiceEc2InstancePolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 août 2023, 13:19 UTC
- Heure modifiée : 03 janvier 2024, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationServiceEc2InstancePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationMigrationServiceRolePolicy

Description : permet au service de migration des AWS applications de créer et de gérer AWS des ressources en votre nom.

AWSApplicationMigrationServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 07 avril 2021, 06:43 UTC
- Heure modifiée : 19 juillet 2026, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationMigrationServiceRolePolicy`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationMigrationSSMAccess

Description : Cette politique donne accès aux opérations Amazon SSM requises pour utiliser Application Migration Service (MGN) afin d'exécuter des documents SSM de commande de post-migration personnalisés. Associez cette politique à vos utilisateurs ou rôles IAM.

AWSApplicationMigrationSSMAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSApplicationMigrationSSMAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 novembre 2022, 09:29 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSApplicationMigrationVCenterClientPolicy

Description : Cette politique permet d'installer et d'utiliser AWS vCenter Client, qui est utilisé avec AWS Application Migration Service (MGN) pour migrer des serveurs externes vers AWS. Attachez cette politique à vos utilisateurs ou rôles IAM dont vous fournissez les informations d'identification lors de l'installation de AWS vCenter Client.

AWSApplicationMigrationVCenterClientPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSElasticMapClientPolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 novembre 2021, 12:53 UTC
- Heure modifiée : 08 novembre 2021, 12:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticMapClientPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAppMeshEnvoyAccess

Description : Politique App Mesh Envoy pour accéder à la configuration du nœud virtuel.

AWSAppMeshEnvoyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSAppMeshEnvoyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 juillet 2019, 21:29 UTC
- Heure modifiée : 3 juillet 2019, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAppMeshFullAccess

Description : fournit un accès complet aux API AWS App Mesh et à la console de gestion.

AWSAppMeshFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSAppMeshFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 16 avril 2019, 17:50 UTC
- Heure modifiée : 07 janvier 2021, 19:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshFullAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAppMeshPreviewEnvoyAccess

Description : Politique App Mesh Preview Envoy pour accéder à la configuration du nœud virtuel.

AWSAppMeshPreviewEnvoyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSAppMeshPreviewEnvoyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 août 2019, 23:32 UTC
- Heure modifiée : 05 août 2019, 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAppMeshPreviewServiceRolePolicy

Description : Permet d'accéder à App Mesh Services AWS et aux ressources utilisées ou gérées par AWS App Mesh

AWSAppMeshPreviewServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 19 juin 2019, 19:07 UTC
- Heure modifiée : 21 août 2019, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
{
  "Sid" : "CloudMapServiceDiscovery",
  "Effect" : "Allow",
  "Action" : [
    "servicediscovery:DiscoverInstances"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ACMCertificateVerification",
  "Effect" : "Allow",
  "Action" : [
    "acm:DescribeCertificate"
  ],
  "Resource" : "*"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAppMeshReadOnly

Description : fournit un accès en lecture seule aux API AWS App Mesh et à la console de gestion.

AWSAppMeshReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSAppMeshReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 16 avril 2019, 17:51 UTC
- Heure modifiée : 07 janvier 2021, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshReadOnly`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"   
}   
]   
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAppMeshServiceRolePolicy

Description : Permet d'accéder Services AWS aux ressources utilisées ou gérées par AWS AppMesh

AWSAppMeshServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 03 juin 2019, 18:30 UTC
- Heure modifiée : 10 octobre 2023, 16:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAppRunnerFullAccess

Description : accorde des autorisations à toutes les actions d'App Runner.

AWSAppRunnerFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSAppRunnerFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 janvier 2022, 04:02 UTC
- Heure modifiée : 11 janvier 2022, 04:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAppRunnerReadOnlyAccess

Description : accorde l'autorisation de répertorier et d'afficher les détails des ressources d'App Runner.

AWSAppRunnerReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSAppRunnerReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 février 2022, 21:24 UTC
- Heure modifiée : 24 février 2022, 21:24 UTC

- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAppRunnerServicePolicyForECRAccess

Description : politique de service AWS App Runner qui accorde des autorisations de lecture aux ressources Amazon ECR du compte du client. Utilisez-le dans un rôle qui est transmis à App Runner lors de la création ou de la mise à jour d'un service App Runner.

AWSAppRunnerServicePolicyForECRAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSAppRunnerServicePolicyForECRAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 14 mai 2021, 19:17 UTC
- Heure modifiée : 14 mai 2021, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAppSyncAdministrator

Description : fournit un accès administratif au AppSync service, mais pas suffisant pour y accéder via la console.

AWSAppSyncAdministratorest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSAppSyncAdministrator à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 mars 2018, 21:20 UTC
- Heure modifiée : 4 novembre 2019, 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncAdministrator`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAppSyncInvokeFullAccess

Description : fournit un accès d'appel complet au AppSync service, à la fois via la console et de manière indépendante

AWSAppSyncInvokeFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSAppSyncInvokeFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 mars 2018, 21:21 UTC
- Heure modifiée : 20 mars 2018, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAppSyncPushToCloudWatchLogs

Description : Permet de AppSync transférer les journaux vers le CloudWatch compte de l'utilisateur.

AWSAppSyncPushToCloudWatchLogsest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSAppSyncPushToCloudWatchLogs à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 09 avril 2018, 19:38 UTC

- Heure modifiée : 09 avril 2018, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAppSyncSchemaAuthor

Description : permet de créer, de mettre à jour et d'interroger le schéma.

AWSAppSyncSchemaAuthor est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSAppSyncSchemaAuthor à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 mars 2018, 21:21 UTC
- Heure modifiée : 01 février 2023, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAppSyncServiceRolePolicy

Description : Permet d'accéder aux AWS services et ressources utilisés ou gérés par AppSync

AWSAppSyncServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 21 janvier 2020, 19:56 UTC
- Heure modifiée : 21 janvier 2020, 19:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSArtifactAccountSync

Description : permet à AWS Artifact d'accéder en lecture seule aux opérations des organisations.
AWS

AWSArtifactAccountSync est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSArtifactAccountSync à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 10 avril 2018, 23:04 UTC
- Heure modifiée : 10 avril 2018, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```



```
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:ListAccounts",
    "organizations:DescribeOrganization"
  ],
  "Resource" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSArtifactAgreementsFullAccess

Description : Cette politique accorde les autorisations complètes pour répertorier, télécharger, accepter et résilier les contrats d' AWS Artifact. Il inclut également les autorisations permettant de répertorier et d'activer AWS l'accès aux services dans le service Organisation, ainsi que de décrire les détails de l'organisation. En outre, la politique permet de vérifier si le rôle lié à un service requis existe et d'en créer un s'il n'existe pas

AWSArtifactAgreementsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSArtifactAgreementsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 novembre 2024, 19:36 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactAgreementsFullAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            ]
        }
    }
}

```

```
]
}
}
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSArtifactAgreementsReadOnlyAccess

Description : Cette politique accorde un accès en lecture seule à la liste des contrats de service AWS Artifact et au téléchargement des contrats acceptés. Il inclut également les autorisations permettant de répertorier et de décrire les détails de l'organisation. En outre, la politique permet de vérifier si le rôle lié à un service requis existe.

AWSArtifactAgreementsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSArtifactAgreementsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 novembre 2024, 19:36 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactAgreementsReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSArtifactComplianceInquiriesFullAccess

Description : fournit un accès complet à l'enquête sur la conformité des artefacts.

AWSArtifactComplianceInquiriesFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSArtifactComplianceInquiriesFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 juin 2026, 19:27 UTC
- Heure modifiée : 30 septembre 2026, 22:47 UTC
- ARN: arn:aws:iam::aws:policy/AWSArtifactComplianceInquiriesFullAccess

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSArtifactComplianceInquiriesReadOnlyAccess

Description : fournit un accès en lecture seule à Artifact Compliance Inquiry.

AWSArtifactComplianceInquiriesReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSArtifactComplianceInquiriesReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 juin 2026, 19:42 UTC
- Heure modifiée : 30 juin 2026, 19:42 UTC
- ARN: arn:aws:iam::aws:policy/AWSArtifactComplianceInquiriesReadOnlyAccess

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSArtifactReportsReadOnlyAccess

Description : fournit un accès en lecture seule aux rapports du service AWS Artifact.

AWSArtifactReportsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSArtifactReportsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 janvier 2024, 22:42 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports",
        "artifact:ListReportVersions"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSArtifactServiceRolePolicy

Description : Permet à AWS Artifact de recueillir des informations sur une organisation via le service AWS Organisations.

AWSArtifactServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 21 août 2023, 20:27 UTC
- Heure modifiée : 21 août 2023, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAuditManagerAdministratorAccess

Description : fournit un accès administratif pour activer ou désactiver AWS Audit Manager, mettre à jour les paramètres et gérer les évaluations, les contrôles et les frameworks

AWSAuditManagerAdministratorAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSAuditManagerAdministratorAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 décembre 2020, 20:02 UTC

- Heure modifiée : 15 mai 2024, 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAuditManagerAdministratorAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAuditManagerServiceRolePolicy

Description : Permet d'accéder aux ressources utilisées ou gérées par AWS Audit Manager Services AWS et de les utiliser

AWSAuditManagerServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 08 décembre 2020, 15:12 UTC
- Heure modifiée : 02 juin 2026, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy`

Version de la politique

Version de la politique : v11 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSAutoScalingPlansEC2AutoScalingPolicy

Description : Politique accordant des autorisations à AWS Auto Scaling pour prévoir périodiquement la capacité et générer des actions de dimensionnement planifiées pour les groupes Auto Scaling dans un plan de dimensionnement

AWSAutoScalingPlansEC2AutoScalingPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 23 août 2018, 22:46 UTC
- Heure modifiée : 23 août 2018, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBackupAccessPointOperatorAccess

Description : Cette politique accorde aux utilisateurs l'autorisation de créer et de gérer des points d'accès de sauvegarde pour accéder aux données de sauvegarde dans les points de restauration via des points d'accès S3.

AWSBackupAccessPointOperatorAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBackupAccessPointOperatorAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 août 2026, 16:12 UTC
- Heure modifiée : 06 août 2026, 16:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupAccessPointOperatorAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBackupAuditAccess

Description : Cette politique autorise les utilisateurs à créer des contrôles et des cadres qui définissent leurs attentes en matière de ressources et d'activités de AWS sauvegarde, et à auditer les ressources et les activités de AWS sauvegarde par rapport aux contrôles et cadres définis.

Cette politique accorde des autorisations à AWS Config et à des services similaires pour décrire les attentes des utilisateurs et effectuer les audits. Cette politique accorde également des autorisations

pour fournir des rapports d'audit à S3 et à des services similaires, et permet aux utilisateurs de rechercher et d'ouvrir leurs rapports d'audit.

AWSBackupAuditAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBackupAuditAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 août 2021, 01:02 UTC
- Heure modifiée : 10 avril 2023, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupAuditAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:::*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBackupDataTransferAccess

Description : Cette politique permet à l'agent AWS Backint d'effectuer le transfert des données de sauvegarde avec le plan de stockage de AWS sauvegarde. Associez cette politique aux rôles assumés par les instances EC2 exécutant SAP HANA avec l'agent Backint.

AWSBackupDataTransferAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBackupDataTransferAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 10 novembre 2022, 22:48 UTC
- Heure modifiée : 10 novembre 2022, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupDataTransferAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBackupFullAccess

Description : Cette politique est destinée aux administrateurs de sauvegarde et accorde un accès complet aux opérations de AWS sauvegarde, y compris la création ou la modification de plans de sauvegarde, l'affectation de AWS ressources aux plans de sauvegarde, la suppression de sauvegardes et la restauration de sauvegardes.

AWSBackupFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBackupFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 novembre 2019, 22:21 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC

- ARN: `arn:aws:iam::aws:policy/AWSBackupFullAccess`

Version de la politique

Version de la politique : v30 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "RedshiftServerlessDeletePermissions",
    "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"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

Description : donne AWS BackupGateway l'autorisation de synchroniser les métadonnées des machines virtuelles en votre nom

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 15 décembre 2022, 19:43 UTC
- Heure modifiée : 15 décembre 2022, 19:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBackupGuardDutyRolePolicyForScans

Description : GuardDuty autorise la lecture de vos points de AWS sauvegarde et de restauration pour les analyses de programmes malveillants

AWSBackupGuardDutyRolePolicyForScans est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSSBackupGuardDutyRolePolicyForScans` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 novembre 2025, 03:34 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSBackupGuardDutyRolePolicyForScans`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBackupOperatorAccess

Description : Cette politique autorise les utilisateurs à affecter des AWS ressources aux plans de sauvegarde, à créer des sauvegardes à la demande et à restaurer des sauvegardes. Cette politique n'autorise pas l'utilisateur à créer ou à modifier des plans de sauvegarde ou à supprimer des sauvegardes planifiées après leur création.

AWSBackupOperatorAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBackupOperatorAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 novembre 2019, 22:23 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOperatorAccess`

Version de la politique

Version de la politique : v28 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBackupOrganizationAdminAccess

Description : Cette politique s'adresse aux administrateurs de sauvegarde qui utilisent la gestion des sauvegardes entre comptes pour gérer les sauvegardes de l'organisation.

AWSBackupOrganizationAdminAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBackupOrganizationAdminAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 juin 2020, 16:23 UTC

- Heure modifiée : 18 novembre 2022, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBackupRestoreAccessForSAPHANA

Description : Fournit l'autorisation de AWS sauvegarde pour restaurer une sauvegarde de SAP HANA sur Amazon EC2

AWSBackupRestoreAccessForSAPHANA est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBackupRestoreAccessForSAPHANA à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 10 novembre 2022, 22:43 UTC
- Heure modifiée : 10 novembre 2022, 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupRestoreAccessForSAPHANA`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*:*:*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBackupSearchOperatorAccess

Description : le rôle d'opérateur de recherche permet de créer des index de sauvegarde, de créer des recherches sur les métadonnées de sauvegarde qui ont été indexées. Cette politique contient les autorisations nécessaires pour ces fonctions d'opérateur de recherche.

AWSBackupSearchOperatorAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBackupSearchOperatorAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 février 2025, 21:52 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupSearchOperatorAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "KMSSDataKeyForSearchAndExportPermissions",
    "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"
  ]
}
}
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBackupServiceLinkedRolePolicyForBackup

Description : fournit l'autorisation AWS de sauvegarde pour créer des sauvegardes en votre nom sur l'ensemble AWS des services

AWSBackupServiceLinkedRolePolicyForBackup est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 02 juin 2020, 23:08 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup`

Version de la politique

Version de la politique : v31 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "RDSInstanceAndSnapshotPermissions",
    "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" : "KMSSDescribePermissions",
    "Effect" : "Allow",
    "Action" : "kms:DescribeKey",
    "Resource" : "*"
},
{
    "Sid" : "KMSGGrantPermissions",
    "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" : "*"
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBackupServiceLinkedRolePolicyForBackupTest

Description : fournit l'autorisation AWS de sauvegarde pour créer des sauvegardes en votre nom sur l'ensemble AWS des services

AWSBackupServiceLinkedRolePolicyForBackupTest est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 12 mai 2020, 17:37 UTC

- Heure modifiée : 12 mai 2020, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  ]
}
```


En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBackupServiceRolePolicyForBackup

Description : fournit l'autorisation AWS de sauvegarde pour créer des sauvegardes en votre nom sur l'ensemble AWS des services

AWSBackupServiceRolePolicyForBackup est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBackupServiceRolePolicyForBackup à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 10 janvier 2019, 21:01 UTC
- Heure modifiée : 23 février 2026, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup`

Version de la politique

Version de la politique : v30 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:eks: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" : "FsxB BackupPermissions",
    "Effect" : "Allow",
    "Action" : "fsx:DescribeBackups",
    "Resource" : "arn:aws:fsx:*:*:backup/*"
},
{
    "Sid" : "FsxCreat BackupPermissions",
    "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"
        }
    }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBackupServiceRolePolicyForIndexing

Description : Politique contenant les autorisations nécessaires pour que AWS Backup indexe les points de restauration.

AWSBackupServiceRolePolicyForIndexing est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBackupServiceRolePolicyForIndexing à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 décembre 2024, 18:37 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForIndexing`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "KMSTDataKeyForEC2Permissions",
    "Effect" : "Allow",
    "Action" : [
      "kms:Decrypt"
    ],
    "Resource" : "arn:aws:kms:*:*:key/*",
    "Condition" : {
      "StringLike" : {
        "kms:ViaService" : [
          "ec2.*.amazonaws.com"
        ]
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBackupServiceRolePolicyForItemRestores

Description : Politique contenant les autorisations nécessaires à AWS Backup pour restaurer des éléments individuels dans un point de restauration

AWSBackupServiceRolePolicyForItemRestores est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBackupServiceRolePolicyForItemRestores à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 décembre 2024, 18:37 UTC
- Heure modifiée : 12 février 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForItemRestores`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "KMSSDataKeyForS3AndEC2Permissions",
    "Effect" : "Allow",
    "Action" : [
      "kms:Decrypt",
      "kms:GenerateDataKey"
    ],
    "Resource" : "arn:aws:kms:*::key/*",
    "Condition" : {
      "StringLike" : {
        "kms:ViaService" : [
          "ec2.*.amazonaws.com",

```

```
        "s3.*.amazonaws.com"  
      ]  
    }  
  }  
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBackupServiceRolePolicyForRestores

Description : fournit l'autorisation AWS de sauvegarde pour effectuer des restaurations en votre nom sur l'ensemble AWS des services. Cette politique inclut des autorisations pour créer et supprimer AWS des ressources, telles que des volumes EBS, des instances RDS et des systèmes de fichiers EFS, qui font partie du processus de restauration.

AWSBackupServiceRolePolicyForRestores est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBackupServiceRolePolicyForRestores à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 12 janvier 2019, 00:23 UTC
- Heure modifiée : 27 août 2026, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForRestores`

Version de la politique

Version de la politique : v36 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "KMSSDescribePermissions",
  "Effect" : "Allow",
  "Action" : "kms:DescribeKey",
  "Resource" : "*"
},
{
  "Sid" : "DSQLResourcePermissionsForRestore",
  "Effect" : "Allow",
  "Action" : [
    "dsq1:StartRestoreJob",
    "dsq1:GetRestoreJob",
    "dsq1:StopRestoreJob",
    "dsq1:TagResource",
    "dsq1>CreateCluster",
    "dsq1:PutMultiRegionProperties",
    "dsq1:PutWitnessRegion",
    "dsq1:UpdateCluster",
    "dsq1:AddPeerCluster",
    "dsq1:RemovePeerCluster",
    "dsq1: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",
                "dsq1.*.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" : "EKSTagOnCreate",
    "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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBackupServiceRolePolicyForS3Backup

Description : Politique contenant les autorisations nécessaires à AWS Backup pour sauvegarder les données dans n'importe quel compartiment S3. Cela inclut l'accès en lecture à tous les objets S3 et tout accès au déchiffrement pour toutes les clés KMS.

AWSBackupServiceRolePolicyForS3Backup est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBackupServiceRolePolicyForS3Backup à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 février 2022, 17:40 UTC
- Heure modifiée : 24 août 2026, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBackupServiceRolePolicyForS3Restore

Description : Politique contenant les autorisations nécessaires à AWS Backup pour restaurer une sauvegarde S3 dans un compartiment. Cela inclut les read/write autorisations pour tous les compartiments S3 et les autorisations DescribeKey pour GenerateDataKey et pour toutes les clés KMS.

AWSBackupServiceRolePolicyForS3Restore est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBackupServiceRolePolicyForS3Restore à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 février 2022, 17:39 UTC
- Heure modifiée : 07 février 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBackupServiceRolePolicyForScans

Description : Fournit l'autorisation AWS de sauvegarde pour effectuer des analyses de programmes malveillants sur vos points AWS de sauvegarde et de restauration

AWSBackupServiceRolePolicyForScans est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBackupServiceRolePolicyForScans à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 novembre 2025, 03:34 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForScans`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBatchFullAccess

Description : fournit un accès complet aux ressources AWS par lots.

AWSBatchFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSBatchFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 décembre 2016, 19:35 UTC
- Heure modifiée : 24 octobre 2022, 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBatchFullAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBatchServiceEventTargetRole

Description : Politique visant à activer CloudWatch Event Target pour la soumission de tâches AWS par lots

AWSBatchServiceEventTargetRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBatchServiceEventTargetRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 28 février 2018, 22:31 UTC
- Heure modifiée : 28 février 2018, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceEventTargetRole`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
    "Action" : [  
        "batch:SubmitJob"  
    ],  
    "Resource" : "*" ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBatchServiceRole

Description : Politique pour le rôle de service AWS Batch qui permet d'accéder aux services associés, notamment EC2, Autoscaling, le service de conteneur EC2 et Cloudwatch Logs.

AWSBatchServiceRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBatchServiceRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 06 décembre 2016, 19:36 UTC
- Heure modifiée : 25 août 2026, 22:27 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole

Version de la politique

Version de la politique : v14 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"  
    }  
  }  
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBatchServiceRolePolicyForSageMaker

Description : permet à AWS Batch d'accéder à la file d'attente et à la gestion des charges SageMaker de travail Amazon

AWSBatchServiceRolePolicyForSageMaker est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 15 juillet 2025, 21:37 UTC
- Heure modifiée : 16 avril 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBatchServiceRolePolicyForSageMaker`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBCMDDataExportsServiceRolePolicy

Description : rôle lié à un service pour permettre aux exportations de données de facturation et de gestion des coûts d'accéder aux données de AWS service afin d'exporter les données vers un emplacement cible, tel qu'Amazon S3, pour le compte d'un client.

AWSBCMDDataExportsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 10 juin 2024, 17:40 UTC
- Heure modifiée : 10 juin 2024, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBCMDDataExportsServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationRecommendationAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBedrockAgentCoreGatewayNetworkServiceRolePolicy

Description : Permet à Bedrock AgentCore Gateway de gérer les ressources VPC Lattice en votre nom

AWSBedrockAgentCoreGatewayNetworkServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 28 mars 2026, 22:12 UTC
- Heure modifiée : 28 mars 2026, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBedrockAgentCoreGatewayNetworkServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBedrockAgentCoreIdentityNetworkServiceRolePolicy

Description : Permet à Bedrock AgentCore Identity de gérer les ressources VPC Lattice en votre nom

AWSBedrockAgentCoreIdentityNetworkServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle

- Heure de création : 15 avril 2026, 00:42 UTC
- Heure modifiée : 15 avril 2026, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBedrockAgentCoreIdentityNetworkServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBedrockAgentCoreRuntimeInstancesServiceRolePolicy

Description : permet aux instances Bedrock AgentCore Runtime de gérer les ressources de calcul en votre nom.

AWSBedrockAgentCoreRuntimeInstancesServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 05 août 2026, 09:57 UTC
- Heure modifiée : 05 août 2026, 09:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBedrockAgentCoreRuntimeInstancesServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBillingConductorFullAccess

Description : utilisez la politique AWSBillingConductorFullAccess gérée pour autoriser un accès complet à la console AWS Billing Conductor (ABC) et aux API. Cette politique permet aux utilisateurs de répertorier, de créer et de supprimer des ressources ABC.

AWSBillingConductorFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBillingConductorFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 avril 2022, 18:02 UTC

- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorFullAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBillingConductorReadOnlyAccess

Description : utilisez la politique AWSBillingConductorReadOnlyAccess gérée pour autoriser l'accès en lecture seule à la console AWS Billing Conductor (ABC) et aux API. Cette politique autorise l'affichage et la liste de toutes les ressources ABC. Il n'inclut pas la possibilité de créer ou de supprimer des ressources.

AWSBillingConductorReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBillingConductorReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 avril 2022, 18:02 UTC
- Heure modifiée : 21 septembre 2026, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBillingConductorRolePolicy

Description : Permet de AWS Billing Conductor gérer les groupes de facturation et les ressources associées

AWSBillingConductorRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 21 septembre 2026, 19:07 UTC
- Heure modifiée : 21 septembre 2026, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBillingConductorRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

```
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBillingReadOnlyAccess

Description : Permet aux utilisateurs de consulter les factures sur la console de facturation.

AWSBillingReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBillingReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 août 2020, 20:08 UTC
- Heure modifiée : 30 juillet 2026, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess`

Version de la politique

Version de la politique : v28 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBillingServiceRolePolicy

Description : Permet au service de facturation de valider l'accès aux données des vues de facturation pour les vues de facturation dérivées

AWSBillingServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 11 septembre 2025, 16:19 UTC
- Heure modifiée : 11 septembre 2025, 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBillingServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
```

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

Description : Cette politique donne des autorisations pour contrôler AWS les ressources. Par exemple, pour démarrer et arrêter des instances EC2 ou RDS en exécutant AWS des scripts Systems Manager (SSM).

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSMest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 mai 2022, 19:03 UTC
- Heure modifiée : 07 avril 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBudgetsActionsWithAWSResourceControlAccess

Description : fournit un accès complet aux actions AWS budgétaires, y compris l'utilisation des actions budgétaires pour contrôler l'état des AWS ressources en cours via Console de gestion AWS

AWSBudgetsActionsWithAWSResourceControlAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBudgetsActionsWithAWSResourceControlAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 octobre 2020, 17:19 UTC
- Heure modifiée : 15 octobre 2020, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActionsWithAWSResourceControlAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBudgetsReadOnlyAccess

Description : fournit un accès en lecture seule à la console AWS Budgets via le Console de gestion AWS.

AWSBudgetsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBudgetsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 octobre 2020, 17:18 UTC

- Heure modifiée : 17 juin 2024, 17:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBudgetsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*",
        "budgets:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBudgetsSpendLimitMemberRolePolicy

Description : accorde au service AWS Budgets les autorisations nécessaires pour décrire, arrêter et résilier les ressources d'un compte membre afin d'appliquer des mesures de limitation des dépenses.

AWSBudgetsSpendLimitMemberRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 18 juillet 2026, 00:57 UTC
- Heure modifiée : 13 août 2026, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBudgetsSpendLimitMemberRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "dsq1:GetCluster",
        "dsq1: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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBugBustFullAccess

Description : Cette politique IAM accorde aux utilisateurs un accès complet à la console AWS BugBust

AWSBugBustFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBugBustFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 juin 2021, 07:03 UTC

- Heure modifiée : 22 juillet 2021, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBugBustPlayerAccess

Description : Cette politique IAM autorise les utilisateurs à participer à AWS BugBust des événements

AWSBugBustPlayerAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSBugBustPlayerAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 juin 2021, 07:15 UTC
- Heure modifiée : 24 juin 2021, 07:15 UTC

- ARN: `arn:aws:iam::aws:policy/AWSBugBustPlayerAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSBugBustServiceRolePolicy

Description : accorde des autorisations AWS BugBust pour accéder aux ressources en votre nom

AWSBugBustServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 24 juin 2021, 06:59 UTC
- Heure modifiée : 24 juin 2021, 06:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCertificateManagerFullAccess

Description : fournit un accès complet au gestionnaire de AWS certificats (ACM)

AWSCertificateManagerFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSCertificateManagerFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 21 janvier 2016, 17:02 UTC
- Heure modifiée : 17 août 2020, 22:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCertificateManagerPrivateCAAuditor

Description : Permet à l'auditeur d'accéder à l'autorité de AWS certification privée du gestionnaire de certificats

AWSCertificateManagerPrivateCAAuditor est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCertificateManagerPrivateCAAuditor à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 octobre 2018, 16:51 UTC
- Heure modifiée : 17 août 2020, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCertificateManagerPrivateCAFullAccess

Description : fournit un accès complet à l'autorité de AWS certification privée du gestionnaire de certificats

AWSCertificateManagerPrivateCAFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCertificateManagerPrivateCAFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 octobre 2018, 16:54 UTC
- Heure modifiée : 23 octobre 2018, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
"Action" : [
  "acm-pca:*"
],
"Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCertificateManagerPrivateCAPrivilegedUser

Description : fournit aux utilisateurs de certificats un accès privilégié à l'autorité de AWS certification privée du gestionnaire de certificats

AWSCertificateManagerPrivateCAPrivilegedUser est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCertificateManagerPrivateCAPrivilegedUser à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 juin 2019, 17:43 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAPrivilegedUser`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCertificateManagerPrivateCAReadOnly

Description : fournit un accès en lecture seule à l'autorité de AWS certification privée du gestionnaire de certificats

AWSCertificateManagerPrivateCAReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCertificateManagerPrivateCAReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 octobre 2018, 16:57 UTC
- Heure modifiée : 17 août 2020, 22:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCertificateManagerPrivateCAUser

Description : Fournit aux utilisateurs du certificat un accès à l'autorité de AWS certification privée du gestionnaire de certificats

AWSCertificateManagerPrivateCAUser est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCertificateManagerPrivateCAUser à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 octobre 2018, 16:53 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCertificateManagerReadOnly

Description : fournit un accès en lecture seule au gestionnaire de AWS certificats (ACM).

AWSCertificateManagerReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCertificateManagerReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 21 janvier 2016, 17:07 UTC
- Heure modifiée : 13 août 2026, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSChatbotServiceLinkedRolePolicy

Description : le rôle lié au service utilisé par le AWS chatbot.

AWSChatbotServiceLinkedRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 18 novembre 2019, 16:39 UTC

- Heure modifiée : 18 novembre 2019, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCleanRoomsFullAccess

Description : Permet un accès complet aux ressources de AWS Clean Rooms et aux ressources connexes Services AWS.

AWSCleanRoomsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCleanRoomsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 janvier 2023, 16:10 UTC
- Heure modifiée : 21 mars 2024, 15:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCleanRoomsFullAccessNoQuerying

Description : Permet un accès complet aux ressources de AWS Clean Rooms, à l'exception des requêtes dans le cadre d'une collaboration et de l'accès aux ressources connexes Services AWS.

AWSCleanRoomsFullAccessNoQuerying est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCleanRoomsFullAccessNoQuerying à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 janvier 2023, 16:12 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCleanRoomsMLFullAccess

Description : Permet un accès complet aux ressources de AWS Clean Rooms ML et l'accès aux ressources connexes Services AWS.

AWSCleanRoomsMLFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCleanRoomsMLFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2023, 21:02 UTC
- Heure modifiée : 12 février 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCleanRoomsMLReadOnlyAccess

Description : autorise un accès en lecture seule aux ressources AWS Clean Rooms ML et un accès en lecture seule aux ressources Clean Rooms associées AWS

AWSCleanRoomsMLReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCleanRoomsMLReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2023, 20:55 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCleanRoomsReadOnlyAccess

Description : autorise un accès en lecture seule aux ressources de AWS Clean Rooms et un accès en lecture seule aux ressources associées à AWS Glue et Amazon Logs. CloudWatch

AWSCleanRoomsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCleanRoomsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 janvier 2023, 16:10 UTC
- Heure modifiée : 12 janvier 2023, 16:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCleanRoomsServiceRolePolicy

Description : Autorisez AWS Clean Rooms à accéder à d'autres AWS services tels que CloudWatch des API en votre nom.

AWSCleanRoomsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 15 décembre 2025, 17:49 UTC
- Heure modifiée : 15 décembre 2025, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCleanRoomsServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "cloudwatch:namespace" : [
      "AWS/Clean Rooms"
    ]
  }
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCloud9Administrator

Description : fournit un accès administrateur à AWS Cloud9.

AWSCloud9Administrator est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCloud9Administrator à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 novembre 2017, 16:17 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9Administrator`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCloud9EnvironmentMember

Description : permet d'être invité dans les environnements de développement partagés AWS Cloud9.

AWSCloud9EnvironmentMember est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSCloud9EnvironmentMember` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 novembre 2017, 16:18 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  ]
}
```



```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCloud9ServiceRolePolicy

Description : Politique relative aux rôles liés aux services pour AWS Cloud9

AWSCloud9ServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 30 novembre 2017, 13:44 UTC
- Heure modifiée : 03 septembre 2026, 23:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCloud9SSMInstanceProfile

Description : Cette politique sera utilisée pour associer un rôle à un InstanceProfile qui permettra à Cloud9 d'utiliser le gestionnaire de session SSM pour se connecter à l'instance

AWSCloud9SSMInstanceProfile est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCloud9SSMInstanceProfile à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 mai 2020, 11:40 UTC
- Heure modifiée : 14 mai 2020, 11:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCloud9User

Description : donne l'autorisation de créer des environnements de développement AWS Cloud9 et de gérer des environnements détenus.

AWSCloud9User est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCloud9User à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 novembre 2017, 16:16 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9User`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCloudFormationFullAccess

Description : fournit un accès complet à AWS CloudFormation.

AWSCloudFormationFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCloudFormationFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 juillet 2019, 21:50 UTC
- Heure modifiée : 26 juillet 2019, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCloudFormationReadOnlyAccess

Description : Permet d'accéder à AWS CloudFormation via le Console de gestion AWS.

AWSCloudFormationReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCloudFormationReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 06 février 2015, 18:39 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:Describe*",
        "cloudformation:BatchDescribe*",
        "cloudformation:EstimateTemplateCost",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "cloudformation:Detect*"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCloudFrontLogger

Description : accorde à CloudFront Logger des autorisations d'écriture sur les CloudWatch journaux.

AWSCloudFrontLogger est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 12 juin 2018, 20:15 UTC
- Heure modifiée : 22 novembre 2019, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
        "logs:CreateLogStream",
        "logs:PutLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCloudFrontVPCOriginServiceRolePolicy

Description : Permet de CloudFront gérer les interfaces réseau Elastic EC2 et les groupes de sécurité en votre nom.

AWSCloudFrontVPCOriginServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 24 octobre 2024, 17:45 UTC
- Heure modifiée : 24 octobre 2024, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontVPCOriginServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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.vpccorigin" : "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" : "*"
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCloudHSMFullAccess

Description : fournit un accès complet à toutes les ressources CloudHSM.

AWSCloudHSMFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCloudHSMFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:39 UTC
- Heure modifiée : 06 février 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCloudHSMReadOnlyAccess

Description : fournit un accès en lecture seule à toutes les ressources CloudHSM.

AWSCloudHSMReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCloudHSMReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:39 UTC
- Heure modifiée : 06 février 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
        "cloudhsm:Get*",
        "cloudhsm:List*",
        "cloudhsm:Describe*"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCloudHSMRole

Description : stratégie par défaut pour le rôle de service AWS CloudHSM.

AWSCloudHSMRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCloudHSMRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 06 février 2015, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCloudMapDiscoverInstanceAccess

Description : donne accès à l'API de découverte de AWS Cloud cartes.

AWSCloudMapDiscoverInstanceAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSCloudMapDiscoverInstanceAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2018, 00:02 UTC
- Heure modifiée : 20 septembre 2023, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCloudMapFullAccess

Description : fournit un accès complet à toutes les actions de AWS Cloud la carte.

AWSCloudMapFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCloudMapFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2018, 23:57 UTC
- Heure modifiée : 29 juillet 2020, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
    "*"
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCloudMapReadOnlyAccess

Description : fournit un accès en lecture seule à toutes les actions AWS Cloud cartographiques.

AWSCloudMapReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCloudMapReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2018, 23:45 UTC
- Heure modifiée : 20 septembre 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCloudMapRegisterInstanceAccess

Description : fournit un accès aux actions de AWS Cloud la carte au niveau du titulaire.

AWSCloudMapRegisterInstanceAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCloudMapRegisterInstanceAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2018, 00:04 UTC
- Heure modifiée : 20 septembre 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
    "*"
  ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCloudShellFullAccess

Description : Subventions à utiliser AWS CloudShell avec toutes les fonctionnalités

AWSCloudShellFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCloudShellFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 15 décembre 2020, 18:07 UTC
- Heure modifiée : 15 décembre 2020, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudShellFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCloudTrail_FullAccess

Description : fournit un accès complet à AWS CloudTrail.

AWSCloudTrail_FullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCloudTrail_FullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 octobre 2020, 23:41 UTC
- Heure modifiée : 22 février 2021, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCloudTrail_ReadOnlyAccess

Description : fournit un accès en lecture seule à AWS CloudTrail.

AWSCloudTrail_ReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCloudTrail_ReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 juin 2022, 17:19 UTC
- Heure modifiée : 14 juin 2022, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
"Effect" : "Allow",
"Action" : [
    "cloudtrail:Get*",
    "cloudtrail:Describe*",
    "cloudtrail:List*",
    "cloudtrail:LookupEvents"
],
"Resource" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

Description : Cette politique est utilisée par le rôle lié à un service nommé `AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents`. CloudWatch utilise ce rôle lié à un service pour exécuter les actions AWS du System Manager Incident Manager lorsqu'une CloudWatch alarme passe à l'état ALARME. Cette politique vous autorise à déclencher des incidents en votre nom.

`AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy` est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 27 avril 2021, 13:30 UTC

- Heure modifiée : 27 avril 2021, 13:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-incidents:StartIncident",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCloudWatchOmniServiceRolePolicy

Description : fournit un accès CloudWatch omnidirectif pour gérer les ressources de l'enregistreur AWS Config, les configurations de télémétrie et les rôles IAM de support pour l'activation de l'organisation.

AWSCloudWatchOmniServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 22 septembre 2026, 05:37 UTC
- Heure modifiée : 24 septembre 2026, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchOmniServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
      }
    }
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodeArtifactAdminAccess

Description : Fournit un accès complet à AWS CodeArtifact via le Console de gestion AWS.

AWSCodeArtifactAdminAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCodeArtifactAdminAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 16 juin 2020, 23:53 UTC
- Heure modifiée : 16 juin 2020, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodeArtifactReadOnlyAccess

Description : Fournit un accès en lecture seule AWS CodeArtifact via le Console de gestion AWS.

AWSCodeArtifactReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCodeArtifactReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 juin 2020, 21:23 UTC
- Heure modifiée : 25 juin 2020, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodeBuildAdminAccess

Description : Fournit un accès complet à AWS CodeBuild via le Console de gestion AWS.

Joignez également AmazonS3ReadOnlyAccess pour accéder au téléchargement des artefacts de construction, et joignez-le IAMFullAccess pour créer et gérer le rôle de service pour CodeBuild.

AWSCodeBuildAdminAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCodeBuildAdminAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2016, 19:04 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess`

Version de la politique

Version de la politique : v20 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodeBuildDeveloperAccess

Description : Fournit un accès AWS CodeBuild via le Console de gestion AWS, mais n'autorise pas l'administration CodeBuild du projet. Joignez également AmazonS3ReadOnlyAccess pour accéder au téléchargement des artefacts de construction.

AWSCodeBuildDeveloperAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSCodeBuildDeveloperAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2016, 19:02 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess`

Version de la politique

Version de la politique : v21 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodeBuildReadOnlyAccess

Description : Fournit un accès en lecture seule AWS CodeBuild via le Console de gestion AWS. Joignez également AmazonS3ReadOnlyAccess pour accéder au téléchargement des artefacts de construction.

AWSCodeBuildReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCodeBuildReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2016, 19:03 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess`

Version de la politique

Version de la politique : v15 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodeCommitFullAccess

Description : Fournit un accès complet à AWS CodeCommit via le Console de gestion AWS.

AWSCodeCommitFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSCodeCommitFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 juillet 2015, 17:02 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitFullAccess`

Version de la politique

Version de la politique : v13 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    }
]

```



```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodeCommitPowerUser

Description : fournit un accès complet aux AWS CodeCommit référentiels, mais n'autorise pas leur suppression.

AWSCodeCommitPowerUser est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCodeCommitPowerUser à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 juillet 2015, 17:06 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitPowerUser`

Version de la politique

Version de la politique : v18 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodeCommitReadOnly

Description : Fournit un accès en lecture seule AWS CodeCommit via le Console de gestion AWS.

AWSCodeCommitReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCodeCommitReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 juillet 2015, 17:05 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitReadOnly`

Version de la politique

Version de la politique : v14 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodeDeployDeployerAccess

Description : donne accès à l'enregistrement et au déploiement d'une révision.

AWSCodeDeployDeployerAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCodeDeployDeployerAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 mai 2015, 18:18 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodeDeployFullAccess

Description : fournit un accès complet aux CodeDeploy ressources.

AWSCodeDeployFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCodeDeployFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 mai 2015, 18:13 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployFullAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodeDeployReadOnlyAccess

Description : fournit un accès en lecture seule aux CodeDeploy ressources.

AWSCodeDeployReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCodeDeployReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 mai 2015, 18:21 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodeDeployRole

Description : fournit un accès au CodeDeploy service permettant d'étendre les balises et d'interagir avec Auto Scaling en votre nom.

AWSCodeDeployRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCodeDeployRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 04 mai 2015, 18:05 UTC
- Heure modifiée : 10 septembre 2026, 10:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodeDeployRoleForCloudFormation

Description : Fournit un accès au CodeDeploy service permettant d'invoquer la fonction Lambda en votre nom pour effectuer blue/green le déploiement. CloudFormation

AWSCodeDeployRoleForCloudFormation est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCodeDeployRoleForCloudFormation à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 19 mai 2020, 17:12 UTC
- Heure modifiée : 19 mai 2020, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodeDeployRoleForECS

Description : fournit un accès à l'ensemble du CodeDeploy service pour effectuer un blue/green déploiement ECS en votre nom. Donne un accès complet aux services de support, tels que l'accès complet pour lire tous les objets S3, invoquer toutes les fonctions Lambda, publier sur toutes les rubriques SNS du compte et mettre à jour tous les services ECS.

AWSCodeDeployRoleForECSe est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCodeDeployRoleForECS à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 27 novembre 2018, 20:40 UTC
- Heure modifiée : 23 septembre 2019, 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ]
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodeDeployRoleForECSLimited

Description : fournit un accès limité au CodeDeploy service pour effectuer un blue/green déploiement ECS en votre nom.

AWSCodeDeployRoleForECSLimited est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCodeDeployRoleForECSLimited à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 novembre 2018, 20:42 UTC
- Heure modifiée : 23 septembre 2019, 22:10 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodeDeployRoleForLambda

Description : fournit un accès au CodeDeploy service pour effectuer un déploiement Lambda en votre nom.

AWSCodeDeployRoleForLambda est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCodeDeployRoleForLambda à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 28 novembre 2017, 14:05 UTC
- Heure modifiée : 03 décembre 2019, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodeDeployRoleForLambdaLimited

Description : fournit un accès limité au CodeDeploy service pour effectuer un déploiement Lambda en votre nom.

AWSCodeDeployRoleForLambdaLimited est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCodeDeployRoleForLambdaLimited à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 17 août 2020, 17:14 UTC
- Heure modifiée : 17 août 2020, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodePipeline_FullAccess

Description : Fournit un accès complet à AWS CodePipeline via le Console de gestion AWS.

AWSCodePipeline_FullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCodePipeline_FullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 août 2020, 22:38 UTC
- Heure modifiée : 14 mars 2024, 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodePipeline_ReadOnlyAccess

Description : Fournit un accès en lecture seule AWS CodePipeline via le Console de gestion AWS.

AWSCodePipeline_ReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCodePipeline_ReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 03 août 2020, 22:25 UTC
- Heure modifiée : 03 août 2020, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodePipelineApproverAccess

Description : Permet de consulter et d'approuver les modifications manuelles pour tous les pipelines

AWSCodePipelineApproverAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCodePipelineApproverAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 28 juillet 2016, 18:59 UTC
- Heure modifiée : 02 août 2017, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:PutApprovalResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodePipelineCustomActionAccess

Description : permet d'accéder à des actions personnalisées permettant de recueillir des informations sur les tâches (y compris des informations d'identification temporaires) et de signaler les mises à jour de statut à AWS CodePipeline.

AWSCodePipelineCustomActionAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCodePipelineCustomActionAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 juillet 2015, 17:02 UTC
- Heure modifiée : 09 juillet 2015, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
```

```
    "codepipeline:PutJobSuccessResult"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
],
"Version" : "2012-10-17"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodeStarFullAccess

Description : Fournit un accès complet à AWS CodeStar via le Console de gestion AWS.

AWSCodeStarFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCodeStarFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 avril 2017, 16:23 UTC
- Heure modifiée : 28 mars 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeStarFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodeStarNotificationsServiceRolePolicy

Description : autorise AWS CodeStar les notifications à accéder à Amazon CloudWatch Events en votre nom

AWSCodeStarNotificationsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 05 novembre 2019, 16:10 UTC
- Heure modifiée : 19 mars 2020, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCodeStarServiceRole

Description : NE PAS UTILISER - Politique de rôle de AWS CodeStar service qui accorde des privilèges administratifs afin de gérer IAM et d'autres ressources de service pour CodeStar le compte du client.

AWSCodeStarServiceRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCodeStarServiceRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 19 avril 2017, 15:20 UTC
- Heure modifiée : 08 septembre 2026, 12:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }

```

```
}  
  }  
] }  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCompromisedKeyQuarantine

Description : Refuse l'accès à certaines actions appliquées par l' AWS équipe dans le cas où les informations d'identification d'un utilisateur IAM auraient été compromises ou exposées publiquement. Ne supprimez PAS cette politique. Veuillez plutôt suivre les instructions spécifiées dans l'e-mail qui vous a été envoyé à propos de cet événement.

AWSCompromisedKeyQuarantineest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCompromisedKeyQuarantine à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 août 2020, 18:04 UTC
- Heure modifiée : 11 août 2020, 18:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "*"
      ]
    }
  ]
}
```

```
]
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCompromisedKeyQuarantineV2

Description : Refuse l'accès à certaines actions appliquées par l' AWS équipe dans le cas où les informations d'identification d'un utilisateur IAM auraient été compromises ou divulguées publiquement. Ne supprimez PAS cette politique. Veuillez plutôt suivre les instructions spécifiées dans le dossier d'assistance créé pour vous concernant cet événement.

AWSCompromisedKeyQuarantineV2est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCompromisedKeyQuarantineV2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 21 avril 2021, 22:30 UTC
- Heure modifiée : 02 octobre 2024, 16:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
    "*"
  ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCompromisedKeyQuarantineV3

Description : Refuse l'accès à certaines actions, appliquées par AWS si les informations d'identification d'un utilisateur IAM ont été compromises ou divulguées publiquement. La politique vise à limiter les dommages potentiels pouvant être causés par des activités liées à la fraude entraînant des frais non autorisés, sans affecter les ressources existantes. Ne supprimez PAS cette politique. Veuillez plutôt suivre les instructions spécifiées dans le dossier d'assistance créé pour vous concernant cet événement.

AWSCompromisedKeyQuarantineV3 est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSCompromisedKeyQuarantineV3` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 21 août 2024, 17:36 UTC
- Heure modifiée : 16 mars 2026, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV3`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSConfigMultiAccountSetupPolicy

Description : Permet à Config d'appeler des AWS services et de déployer des ressources de configuration dans l'ensemble de l'organisation

AWSConfigMultiAccountSetupPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 17 juin 2019, 18:03 UTC

- Heure modifiée : 24 février 2023, 01:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"  
    }  
  }  
}  
]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSConfigRemediationServiceRolePolicy

Description : permet à AWS Config de corriger les ressources non conformes pour vous.

AWSConfigRemediationServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 18 juin 2019, 21:21 UTC
- Heure modifiée : 18 juin 2019, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSConfigRoleForOrganizations

Description : permet à AWS Config d'appeler les API des organisations en lecture seule AWS

AWSConfigRoleForOrganization est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSConfigRoleForOrganizations` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 19 mars 2018, 22:53 UTC
- Heure modifiée : 24 novembre 2020, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSConfigRulesExecutionRole

Description : permet à une fonction AWS Lambda d'accéder à l'API AWS Config et aux instantanés de configuration que AWS Config fournit périodiquement à Amazon S3. Cet accès est requis par les fonctions qui évaluent les modifications de configuration pour les règles de configuration personnalisées.

AWSConfigRulesExecutionRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSConfigRulesExecutionRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 25 mars 2016, 17:59 UTC
- Heure modifiée : 13 mai 2019, 21:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSConfigServiceRolePolicy

Description : permet à Config d'appeler AWS des services et de collecter des configurations de ressources en votre nom.

AWSConfigServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 30 mai 2018, 23:31 UTC
- Heure modifiée : 23 septembre 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy`

Version de la politique

Version de la politique : v96 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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",
"dsq1:GetCluster",
"dsq1:GetClusterPolicy",
"dsq1:GetVpcEndpointServiceName",
"dsq1:ListClusters",
"dsq1: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:GetFirmwareTask",
"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:DescribeVPCCConnection",
"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:ListVPCCConnections",
"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:ListModel",
"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:DescribeSenderId",
"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/*"
  ]
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSConfigThirdPartyServiceRolePolicy

Description : autorise AWS Config à inventorier et à évaluer la conformité des ressources cloud tierces.

AWSConfigThirdPartyServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 22 juin 2026, 17:57 UTC
- Heure modifiée : 22 juin 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigThirdPartyServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSConfigUserAccess

Description : donne accès à l'utilisation de AWS Config, notamment à la recherche par balises sur les ressources et à la lecture de toutes les balises. Cela ne donne pas l'autorisation de configurer AWS Config, qui nécessite des privilèges administratifs.

AWSConfigUserAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSConfigUserAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 février 2015, 19:38 UTC
- Heure modifiée : 18 mars 2019, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConfigUserAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

Connecteur AWS

Description : Permet un read/write accès étendu à TOUS les objets EC2, l' read/write accès aux compartiments S3 commençant par « import-to-ec2- » et la possibilité de répertorier tous les compartiments S3, afin que le AWS connecteur puisse importer des machines virtuelles en votre nom.

AWSConnector est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSConnector à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 février 2015, 17:14 UTC
- Heure modifiée : 28 septembre 2015, 19:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConnector`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
}

```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSControlTowerAccountServiceRolePolicy

Description : Permet à AWS Control Tower d'appeler AWS des services qui fournissent une configuration automatique des comptes et une gouvernance centralisée en votre nom.

AWSControlTowerAccountServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 05 juin 2023, 22:04 UTC
- Heure modifiée : 20 mai 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy`

Version de la politique

Version de la politique : v11 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSControlTowerCloudTrailRolePolicy

Description : AWS Control Tower active AWS CloudTrail en tant que meilleure pratique et confère ce rôle à AWS CloudTrail. AWS CloudTrail assume ce rôle pour créer et publier des CloudTrail journaux

AWSControlTowerCloudTrailRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSControlTowerCloudTrailRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 05 novembre 2025, 21:19 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSControlTowerCloudTrailRolePolicy

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*:*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSControlTowerIdentityCenterManagementPolicy

Description : fournit les autorisations nécessaires pour gérer les ressources IAM Identity Center (iDC) dans les comptes membres inscrits à AWS Control Tower. La politique est associée au AWSControlTowerAdmin rôle uniquement si le client a choisi l'intégration IAM iDC dans sa AWS zone d'atterrissage de la tour de contrôle.

AWSControlTowerIdentityCenterManagementPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSControlTowerIdentityCenterManagementPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 03 octobre 2025, 18:34 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerIdentityCenterManagementPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSControlTowerServiceRolePolicy

Description : Permet d'accéder aux AWS ressources gérées ou utilisées par AWS Control Tower

AWSControlTowerServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSControlTowerServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 03 mai 2019, 18:19 UTC
- Heure modifiée : 10 septembre 2026, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy`

Version de la politique

Version de la politique : v22 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            ]
        }
    }
}
}

```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSCostAndUsageReportAutomationPolicy

Description : accorde des autorisations permettant de décrire l'organisation du compte, de créer des compartiments S3 pour le programme MAP et d'y appliquer des balises, de créer un rapport sur les coûts et l'utilisation et de décrire les définitions des rapports de coûts et d'utilisation.

AWSCostAndUsageReportAutomationPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSCostAndUsageReportAutomationPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 01 novembre 2021, 21:27 UTC
- Heure modifiée : 01 novembre 2021, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDataExchangeDataGrantOwnerFullAccess

Description : permet aux titulaires de Data Grant d'accéder aux actions AWS Data Exchange à l'aide du SDK Console de gestion AWS et.

AWSDataExchangeDataGrantOwnerFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDataExchangeDataGrantOwnerFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 octobre 2024, 14:43 UTC
- Heure modifiée : 24 octobre 2024, 14:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeDataGrantOwnerFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      ]
    }
  }
}
]
}
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDataExchangeDataGrantReceiverFullAccess

Description : permet au destinataire de Data Grant d'accéder aux actions AWS Data Exchange à l'aide du SDK Console de gestion AWS et.

AWSDataExchangeDataGrantReceiverFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDataExchangeDataGrantReceiverFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 octobre 2024, 14:45 UTC
- Heure modifiée : 24 octobre 2024, 14:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeDataGrantReceiverFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDataExchangeFullAccess

Description : accorde un accès complet à AWS Data Exchange et aux AWS Marketplace actions à l'aide du SDK Console de gestion AWS et. Il fournit également un accès sélectif aux services connexes nécessaires pour tirer pleinement parti de l'échange de AWS données.

AWSDataExchangeFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDataExchangeFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 novembre 2019, 19:27 UTC
- Heure modifiée : 24 juin 2024, 19:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeFullAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDataExchangeProviderFullAccess

Description : accorde aux fournisseurs de données l'accès à AWS Data Exchange et aux AWS Marketplace actions à l'aide du SDK Console de gestion AWS et. Il fournit également un accès sélectif aux services connexes nécessaires pour tirer pleinement parti de l'échange de AWS données.

AWSDataExchangeProviderFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDataExchangeProviderFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 novembre 2019, 19:27 UTC
- Heure modifiée : 15 août 2024, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDataExchangeReadOnly

Description : accorde un accès en lecture seule à AWS Data Exchange et aux AWS Marketplace actions à l'aide du SDK Console de gestion AWS et.

AWSDataExchangeReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDataExchangeReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 novembre 2019, 19:27 UTC
- Heure modifiée : 24 octobre 2024, 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeReadOnly`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDataExchangeServiceRolePolicyForLicenseManagement

Description : permet à AWS Data Exchange d'accéder Services AWS aux ressources utilisées ou gérées par AWS Data Exchange pour la gestion des licences.

AWSDataExchangeServiceRolePolicyForLicenseManagement est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 10 octobre 2024, 14:54 UTC
- Heure modifiée : 10 octobre 2024, 14:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataExchangeServiceRolePolicyForLicenseManagement`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDataExchangeServiceRolePolicyForOrganizationDiscovery

Description : permet à AWS Data Exchange de lire les données relatives à votre AWS organisation afin de déterminer l'éligibilité à la distribution de licences AWS Data Exchange.

AWSDataExchangeServiceRolePolicyForOrganizationDiscovery est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 10 octobre 2024, 14:33 UTC
- Heure modifiée : 10 octobre 2024, 14:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataExchangeServiceRolePolicyForOrganizationDiscovery`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAWSOrganizationsActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDataExchangeSubscriberFullAccess

Description : permet aux abonnés de données d'accéder à AWS Data Exchange et aux AWS Marketplace actions à l'aide du SDK Console de gestion AWS et. Il fournit également un accès sélectif aux services connexes nécessaires pour tirer pleinement parti de l'échange de AWS données.

AWSDataExchangeSubscriberFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDataExchangeSubscriberFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 novembre 2019, 19:27 UTC
- Heure modifiée : 21 mai 2024, 17:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDatalifecycleManagerServiceRole

Description : fournit les autorisations appropriées à AWS Data Lifecycle Manager pour qu'il puisse prendre des mesures sur les AWS ressources

AWSDatalifecycleManagerServiceRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDatalifecycleManagerServiceRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 06 juillet 2018, 19:34 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDatalifecycleManagerServiceRole`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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.*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDataLifecycleManagerServiceRoleForAMIManagement

Description : fournit les autorisations appropriées à AWS Data Lifecycle Manager pour prendre des mesures sur les AWS ressources pour la gestion des AMI

AWSDataLifecycleManagerServiceRoleForAMIManagement est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDataLifecycleManagerServiceRoleForAMIManagement à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 21 octobre 2020, 19:39 UTC
- Heure modifiée : 19 août 2021, 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRoleForAMIManagement`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDataLifecycleManagerSSMFullAccess

Description : fournit à Amazon Data Lifecycle Manager l'autorisation d'effectuer les actions de Systems Manager requises pour exécuter les pré-scripts et les post-scripts sur toutes les instances Amazon EC2.

AWSDataLifecycleManagerSSMFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDataLifecycleManagerSSMFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 31 octobre 2023, 20:29 UTC
- Heure modifiée : 16 novembre 2023, 22:31 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerSSMFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
      ]
    }
  ]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDatapipeline_FullAccess

Description : fournit un accès complet au pipeline de données, un accès à la liste pour les rôles S3, DynamoDB, Redshift, RDS, SNS et IAM, et un accès PassRole pour les rôles par défaut.

AWSDatapipeline_FullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSDatapipeline_FullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 janvier 2017, 23:14 UTC
- Heure modifiée : 17 août 2017, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDatapipeline_FullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDataPipeline_PowerUser

Description : fournit un accès complet au pipeline de données, un accès à la liste pour les rôles S3, DynamoDB, Redshift, RDS, SNS et IAM, et un accès PassRole pour les rôles par défaut.

AWSDataPipeline_PowerUser est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDataPipeline_PowerUser à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 janvier 2017, 23:16 UTC

- Heure modifiée : 17 août 2017, 18:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataPipeline_PowerUser

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDDataSyncDiscoveryServiceRolePolicy

Description : permet à DataSync Discovery de s'intégrer à d'autres AWS services en votre nom.

AWSDDataSyncDiscoveryServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 20 mars 2023, 22:19 UTC
- Heure modifiée : 20 mars 2023, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDDataSyncDiscoveryServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*"
      ]
    }
  ]
}
```

```
]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDDataSyncFullAccess

Description : fournit un accès complet AWS DataSync et un accès minimal à ses dépendances

AWSDDataSyncFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDDataSyncFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 janvier 2019, 19:40 UTC
- Heure modifiée : 12 février 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDDataSyncFullAccess`

Version de la politique

Version de la politique : v16 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDDataSyncReadOnlyAccess

Description : fournit un accès en lecture seule à AWS DataSync

AWSDDataSyncReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDDataSyncReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 janvier 2019, 19:18 UTC
- Heure modifiée : 30 juin 2020, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDDataSyncReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDDataSyncServiceRolePolicy

Description : Permet DataSync l'intégration à d'autres AWS services en votre nom

AWSDDataSyncServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 09 octobre 2024, 17:45 UTC
- Heure modifiée : 15 avril 2025, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDDataSyncServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
      }
    }
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDeadlineCloud-FleetWorker

Description : permet aux employés de AWS Deadline Cloud d'accéder à des tâches sur une ferme de serveurs.

AWSDeadlineCloud-FleetWorker est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDeadlineCloud-FleetWorker à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 avril 2024, 17:21 UTC
- Heure modifiée : 01 avril 2024, 17:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-FleetWorker`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
    }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDeadlineCloud-UserAccessFarms

Description : Fournit aux stations de travail des utilisateurs un accès aux fermes AWS Deadline Cloud avec Read-Only des autorisations limitées pour appeler les autres services nécessaires. Associez cette politique au rôle d'utilisateur associé à votre studio.

AWSDeadlineCloud-UserAccessFarmsest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDeadlineCloud-UserAccessFarms à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 avril 2024, 16:54 UTC
- Heure modifiée : 29 mai 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFarms`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDeadlineCloud-UserAccessFleets

Description : Fournit aux postes de travail des utilisateurs un accès aux flottes AWS Deadline Cloud avec Read-Only des autorisations limitées pour appeler les autres services nécessaires. Associez cette politique au rôle d'utilisateur associé à votre studio.

AWSDeadlineCloud-UserAccessFleets est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDeadlineCloud-UserAccessFleets à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 avril 2024, 17:01 UTC

- Heure modifiée : 29 mai 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFleets`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDeadlineCloud-UserAccessJobs

Description : Fournit aux postes de travail des utilisateurs un accès aux tâches AWS Deadline Cloud avec Read-Only des autorisations limitées pour appeler les autres services nécessaires. Associez cette politique au rôle d'utilisateur associé à votre studio.

AWSDeadlineCloud-UserAccessJobs est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDeadlineCloud-UserAccessJobs à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 avril 2024, 17:05 UTC
- Heure modifiée : 07 octobre 2024, 18:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessJobs`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
            }
        }
    }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDeadlineCloud-UserAccessQueues

Description : fournit aux postes de travail des utilisateurs un accès aux files d'attente de AWS Deadline Cloud avec Read-Only des autorisations limitées pour appeler les autres services nécessaires. Associez cette politique au rôle d'utilisateur associé à votre studio.

AWSDeadlineCloud-UserAccessQueues est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDeadlineCloud-UserAccessQueues à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 avril 2024, 17:10 UTC
- Heure modifiée : 07 octobre 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessQueues`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"  
}  
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDeadlineCloud-WorkerHost

Description : permet aux hôtes travailleurs de AWS Deadline Cloud de rejoindre une flotte dans une ferme.

AWSDeadlineCloud-WorkerHost est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDeadlineCloud-WorkerHost à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 avril 2024, 17:28 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-WorkerHost`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDeepLensLambdaFunctionAccessPolicy

Description : cette politique spécifie les autorisations requises par les fonctions Lambda d' DeepLens administration qui s'exécutent sur un appareil DeepLens

AWSDeepLensLambdaFunctionAccessPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDeepLensLambdaFunctionAccessPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2017, 15:47 UTC
- Heure modifiée : 11 juin 2019, 23:11 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
            "*"
        ]
    }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDeepLensServiceRolePolicy

Description : donne AWS DeepLens accès aux ressources et aux rôles nécessaires Services AWS, DeepLens ainsi qu'à leurs dépendances, notamment IoT, S3 GreenGrass et AWS Lambda.

AWSDeepLensServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDeepLensServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service

- Heure de création : 29 novembre 2017, 15:46 UTC
- Heure modifiée : 25 septembre 2019, 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
      "*"
    ]
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDeepRacerAccountAdminAccess

Description : accès DeepRacer administrateur à toutes les actions, y compris le basculement entre le mode multi-utilisateur et le mode mono-utilisateur.

AWSDeepRacerAccountAdminAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDeepRacerAccountAdminAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 octobre 2021, 01:27 UTC
- Heure modifiée : 28 octobre 2021, 01:27 UTC

- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepRacerAdminAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "true"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDeepRacerCloudFormationAccessPolicy

Description : Permet CloudFormation de créer et de gérer des AWS piles et des ressources en votre nom.

AWSDeepRacerCloudFormationAccessPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDeepRacerCloudFormationAccessPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 février 2019, 21:59 UTC
- Heure modifiée : 14 juin 2019, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDeepRacerDefaultMultiUserAccess

Description : Accès utilisateur DeepRacer MultiUser par défaut pour utiliser deepracer en mode multi-utilisateurs

AWSDeepRacerDefaultMultiUserAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSDeepRacerDefaultMultiUserAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 octobre 2021, 01:27 UTC
- Heure modifiée : 28 octobre 2021, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "*"
    ]
}
]
}

```


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDeepRacerFullAccess

Description : fournit un accès complet à AWS DeepRacer. Fournit également un accès sélectif à des services connexes (par exemple, S3).

AWSDeepRacerFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDeepRacerFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 octobre 2020, 22:03 UTC
- Heure modifiée : 05 octobre 2020, 22:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*/*"
    ]
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDeepRacerRoboMakerAccessPolicy

Description : Permet RoboMaker de créer les ressources nécessaires et d'appeler AWS les services en votre nom.

AWSDeepRacerRoboMakerAccessPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDeepRacerRoboMakerAccessPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 février 2019, 21:59 UTC
- Heure modifiée : 28 février 2019, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDeepRacerServiceRolePolicy

Description : Permet DeepRacer de créer les ressources nécessaires et d'appeler AWS les services en votre nom.

AWSDeepRacerServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSDeepRacerServiceRolePolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 28 février 2019, 21:58 UTC
- Heure modifiée : 12 juin 2019, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDenyAll

Description : Refuser tout accès.

AWSDenyAll est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDenyAll à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 mai 2019, 22:36 UTC
- Heure modifiée : 18 décembre 2023, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDenyAll`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDeviceFarmFullAccess

Description : fournit un accès complet à toutes les opérations de AWS Device Farm.

AWSDeviceFarmFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDeviceFarmFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 juillet 2015, 16:37 UTC
- Heure modifiée : 13 juillet 2015, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDDeviceFarmServiceRolePolicy

Description : accordez à AWS Device Farm l'autorisation d'appeler les API réseau EC2 en votre nom.

AWSDDeviceFarmServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 20 septembre 2022, 21:02 UTC
- Heure modifiée : 20 septembre 2022, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDDeviceFarmServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]

```

```
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDeviceFarmTestGridServiceRolePolicy

Description : accordez à AWS Device Farm l'autorisation d'appeler les API EC2 en votre nom.

AWSDeviceFarmTestGridServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 26 mai 2021, 22:01 UTC
- Heure modifiée : 26 mai 2021, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDirectConnectFullAccess

Description : Fournit un accès complet à AWS Direct Connect via le Console de gestion AWS.

AWSDirectConnectFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDirectConnectFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 30 avril 2019, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
    "directconnect:*",
    "ec2:DescribeVpnGateways",
    "ec2:DescribeTransitGateways"
  ],
  "Resource" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDirectConnectReadOnlyAccess

Description : Fournit un accès en lecture seule à AWS Direct Connect via le Console de gestion AWS.

AWSDirectConnectReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDirectConnectReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 18 mai 2020, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:Describe*",
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDirectConnectServiceRolePolicy

Description : fournit l'autorisation AWS Direct Connect de créer et de gérer AWS des ressources en votre nom.

AWSDirectConnectServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 14 janvier 2021, 18:35 UTC
- Heure modifiée : 14 janvier 2021, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*directconnect*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDirectoryServiceDataFullAccess

Description : fournit un accès complet aux données AWS du service d'annuaire.

AWSDirectoryServiceDataFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDirectoryServiceDataFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 septembre 2024, 21:45 UTC
- Heure modifiée : 18 septembre 2024, 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceDataFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDirectoryServiceDataReadOnlyAccess

Description : fournit un accès en lecture seule aux données du service d' AWS annuaire

AWSDirectoryServiceDataReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDirectoryServiceDataReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 septembre 2024, 22:00 UTC
- Heure modifiée : 18 septembre 2024, 22:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceDataReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDirectoryServiceFullAccess

Description : fournit un accès complet au service d' AWS annuaire.

AWSDirectoryServiceFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDirectoryServiceFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 02 avril 2024, 20:38 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDirectoryServiceReadOnlyAccess

Description : fournit un accès en lecture seule au service d' AWS annuaire.

AWSDirectoryServiceReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDirectoryServiceReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 25 septembre 2018, 21:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDirectoryServiceServiceRolePolicy

Description : Politique relative au rôle lié au service d'annuaire

AWSDirectoryServiceServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle

- Heure de création : 11 juillet 2025, 00:22 UTC
- Heure modifiée : 11 juillet 2025, 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectoryServiceServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDiscoveryContinuousExportFirehosePolicy

Description : fournit un accès en écriture aux AWS ressources requises pour AWS Discovery Continuous Export

AWSDiscoveryContinuousExportFirehosePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSDiscoveryContinuousExportFirehosePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 août 2018, 18:29 UTC
- Heure modifiée : 08 juin 2021, 17:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*"
      ]
    }
  ]
}
```



```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDMSFleetAdvisorServiceRolePolicy

Description : Permet à DMS Fleet Advisor de gérer les CloudWatch indicateurs en votre nom.

AWSDMSFleetAdvisorServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 06 mars 2023, 09:10 UTC
- Heure modifiée : 06 mars 2023, 09:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSFleetAdvisorServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/DMS/FleetAdvisor"
      }
    }
  }
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSDMSServerlessServiceRolePolicy

Description : accorde les autorisations AWS DMS Serverless pour créer et gérer les ressources DMS de votre compte en votre nom

AWSDMSServerlessServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 18 mai 2023, 20:28 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
      }
    }
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSEC2CapacityManagerServiceRolePolicy

Description : permet à EC2 Capacity Manager de gérer les ressources de capacité et de s'intégrer aux AWS organisations en votre nom.

AWSEC2CapacityManagerServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 09 octobre 2025, 22:04 UTC
- Heure modifiée : 09 octobre 2025, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityManagerServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSEC2CapacityReservationFleetRolePolicy

Description : Permet au service EC2 CapacityReservation Fleet de gérer les réservations de capacité

AWSEC2CapacityReservationFleetRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 29 septembre 2021, 14:43 UTC
- Heure modifiée : 03 mars 2025, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSEC2FleetServiceRolePolicy

Description : Permet à EC2 Fleet de lancer et de gérer des instances.

AWSEC2FleetServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 21 mars 2018, 00:08 UTC
- Heure modifiée : 04 mai 2020, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
      }
    }
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSEC2SpotFleetServiceRolePolicy

Description : Permet à EC2 Spot Fleet de lancer et de gérer des instances de flotte ponctuelle

AWSEC2SpotFleetServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 23 octobre 2017, 19:13 UTC
- Heure modifiée : 16 mars 2020, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*:*:*/*"
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSEC2SpotServiceRolePolicy

Description : Permet à EC2 Spot de lancer et de gérer des instances ponctuelles

AWSEC2SpotServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 18 septembre 2017, 18:51 UTC
- Heure modifiée : 12 décembre 2018, 00:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSEC2SqlHaInstancePolicy

Description : autorisations d'instance Amazon EC2 permettant au service EC2 SQL High Availability de détecter l'état de haute disponibilité de l'instance via le profil d'instance EC2.

AWSEC2SqlHaInstancePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSEC2SqlHaInstancePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 novembre 2025, 01:49 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEC2SqlHaInstancePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSEC2SqlHaServiceRolePolicy

Description : Autorisations du service EC2 SQL High Availability pour détecter les instances standby/passive

AWSEC2SqlHaServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 13 novembre 2025, 01:34 UTC
- Heure modifiée : 13 novembre 2025, 01:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SqlHaServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSEC2VssRestorePolicy

Description : accorde les autorisations Amazon EC2 et AWS SSM pour restaurer la base de données SQL Server à partir d'instantanés cohérents avec les applications créés par VSS. AWS

AWSEC2VssRestorePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSEC2VssRestorePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 mars 2026, 23:12 UTC
- Heure modifiée : 25 mars 2026, 23:12 UTC
- ARN: arn:aws:iam::aws:policy/AWSEC2VssRestorePolicy

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ]
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSEC2VssSnapshotPolicy

Description : Cette politique est associée au rôle IAM associé à vos instances Windows Amazon EC2 afin de permettre à la solution Amazon EC2 VSS de créer et d'ajouter des balises à Amazon Machine Images (AMI) et EBS Snapshots.

AWSEC2VssSnapshotPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSEC2VssSnapshotPolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 mars 2024, 16:32 UTC
- Heure modifiée : 20 novembre 2024, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEC2VssSnapshotPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSECRPullThroughCache_ServiceRolePolicy

Description : Permet d'accéder aux AWS services et aux ressources utilisés ou gérés par AWS ECR Pull Through Cache

AWSECRPullThroughCache_ServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 26 novembre 2021, 21:51 UTC
- Heure modifiée : 12 mai 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
    }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticBeanstalkCustomPlatformforEC2Role

Description : dans votre environnement de création de plateforme personnalisé, autorisez l'instance à lancer l'instance EC2, à créer un instantané EBS et une AML, à diffuser des journaux vers Amazon CloudWatch Logs et à stocker des artefacts dans Amazon S3.

AWSElasticBeanstalkCustomPlatformforEC2Role est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticBeanstalkCustomPlatformforEC2Role à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 21 février 2017, 22:50 UTC
- Heure modifiée : 21 février 2017, 22:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticBeanstalkEKSIImageBuild

Description : autorisations requises par Elastic Beanstalk pour créer des images de conteneurs pour le compte du client.

AWSElasticBeanstalkEKSIImageBuild est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticBeanstalkEKSIImageBuild à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 juillet 2026, 21:27 UTC
- Heure modifiée : 02 juillet 2026, 21:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkEKSIImageBuild

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  }
}
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticBeanstalkEKSObservability

Description : autorisations d'observabilité pour les environnements Elastic Beanstalk exécutés dans le cluster Elastic Kubernetes Service

AWSElasticBeanstalkEKSObservability est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticBeanstalkEKSObservability à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 juillet 2026, 21:27 UTC
- Heure modifiée : 02 juillet 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkEKSObservability`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticBeanstalkEKSTagging

Description : autorisations nécessaires pour transmettre des balises aux ressources créées par les contrôleurs EKS

AWSElasticBeanstalkEKSTagging est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSElasticBeanstalkEKSTagging` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 juillet 2026, 21:27 UTC
- Heure modifiée : 02 juillet 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkEKSTagging`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticBeanstalkEnhancedHealth

Description : Politique du service AWS Elastic Beanstalk pour le système de surveillance de l'état

AWSElasticBeanstalkEnhancedHealth est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticBeanstalkEnhancedHealth à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 08 février 2016, 23:17 UTC
- Heure modifiée : 09 avril 2018, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticBeanstalkMaintenance

Description : politique AWS Elastic Beanstalk Service Role qui accorde des autorisations limitées pour mettre à jour vos ressources en votre nom à des fins de maintenance.

AWSElasticBeanstalkMaintenance est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 11 janvier 2019, 23:22 UTC
- Heure modifiée : 29 avril 2024, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

Description : Cette politique concerne le rôle de service AWS Elastic Beanstalk utilisé pour effectuer des mises à jour gérées des environnements Elastic Beanstalk. Cette politique ne doit pas être associée à d'autres utilisateurs ou rôles. La politique accorde des autorisations étendues pour créer et gérer des ressources sur un certain nombre de AWS services AutoScaling, notamment EC2, ECS, Elastic Load Balancing et CloudFormation. Cette politique permet également de transmettre tout rôle IAM utilisable avec ces services.

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 mars 2021, 22:18 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      ]
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

Description : politique AWS Elastic Beanstalk Service Role qui accorde des autorisations limitées aux mises à jour gérées.

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 21 novembre 2019, 22:35 UTC
- Heure modifiée : 13 mars 2026, 16:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
]
```

```
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticBeanstalkMulticontainerDocker

Description : Fournissez aux instances de votre environnement Docker multiconteneurs l'accès pour utiliser Amazon EC2 Container Service afin de gérer les tâches de déploiement de conteneurs.

AWSElasticBeanstalkMulticontainerDocker est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticBeanstalkMulticontainerDocker à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 février 2016, 23:15 UTC
- Heure modifiée : 29 avril 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "AIEEnvironmentAnalysisInvokeFoundationModel",
    "Effect" : "Allow",
    "Action" : "bedrock:InvokeModel",
    "Resource" : [
      "arn:aws:bedrock:*::foundation-model/anthropic.claude-*",
      "arn:aws:bedrock:*::foundation-model/amazon.nova-*"
    ]
  },
  {

```

```

    "Sid" : "AIEEnvironmentAnalysisInvokeInferenceProfile",
    "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" : "AIEEnvironmentAnalysisReadOnly",
    "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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticBeanstalkReadOnly

Description : accorde des autorisations en lecture seule. Permet explicitement aux opérateurs d'accéder directement aux informations relatives aux ressources liées aux applications AWS Elastic Beanstalk.

AWSElasticBeanstalkReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticBeanstalkReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 janvier 2021, 19:02 UTC
- Heure modifiée : 19 mai 2026, 13:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*"
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticBeanstalkRoleCore

Description : AWSElasticBeanstalkRoleCore (rôle opérationnel d'Elastic Beanstalk) Permet le fonctionnement de base d'un environnement de service Web.

AWSElasticBeanstalkRoleCore est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticBeanstalkRoleCore à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 05 juin 2020, 21:48 UTC
- Heure modifiée : 30 avril 2024, 00:01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "S30bj",
    "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"
            ]
        }
    }
}
]
}
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticBeanstalkRoleCWL

Description : (rôle opérationnel d'Elastic Beanstalk) Permet à un environnement de gérer les groupes de CloudWatch journaux Amazon Logs.

AWSElasticBeanstalkRoleCWL est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticBeanstalkRoleCWL à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 05 juin 2020, 21:49 UTC
- Heure modifiée : 05 juin 2020, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticBeanstalkRoleECS

Description : (rôle opérationnel d'Elastic Beanstalk) Permet à un environnement Docker multiconteneurs de gérer les clusters Amazon ECS.

AWSElasticBeanstalkRoleECS est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticBeanstalkRoleECS à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 05 juin 2020, 21:47 UTC
- Heure modifiée : 23 mars 2023, 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
          ]
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticBeanstalkRoleRDS

Description : (rôle opérationnel d'Elastic Beanstalk) Permet à un environnement d'intégrer une instance Amazon RDS.

AWSElasticBeanstalkRoleRDS est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticBeanstalkRoleRDS à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 05 juin 2020, 21:46 UTC
- Heure modifiée : 05 juin 2020, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticBeanstalkRoleSNS

Description : (rôle opérationnel d'Elastic Beanstalk) Permet de créer un environnement permettant l'intégration des rubriques Amazon SNS.

AWSElasticBeanstalkRoleSNS est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticBeanstalkRoleSNS à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 05 juin 2020, 21:46 UTC
- Heure modifiée : 05 juin 2020, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"    
  }  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticBeanstalkRoleWorkerTier

Description : (rôle opérationnel d'Elastic Beanstalk) Permet à un niveau d'environnement de travail de créer une table Amazon DynamoDB et une file d'attente Amazon SQS.

AWSElasticBeanstalkRoleWorkerTier est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticBeanstalkRoleWorkerTier à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 05 juin 2020, 21:43 UTC
- Heure modifiée : 05 juin 2020, 21:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticBeanstalkService

Description : Cette politique est sur la voie de la dépréciation. Consultez la documentation pour obtenir des conseils : Politique de rôle d'<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/iam-servicerole.html>. AWS Elastic Beanstalk Service qui accorde des autorisations pour créer et gérer des ressources (par exemple : AutoScaling EC2, S3, ELB CloudFormation, etc.) en votre nom.

AWSElasticBeanstalkService est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticBeanstalkService à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 11 avril 2016, 20:27 UTC
- Heure modifiée : 10 mai 2023, 19:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService`

Version de la politique

Version de la politique : v17 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
    "*"
  ]
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticBeanstalkServiceRolePolicy

Description : politique AWS Elastic Beanstalk Service Linked Role qui accorde des autorisations pour créer et gérer des ressources (par exemple : AutoScaling EC2, S3, ELB CloudFormation, etc.) en votre nom.

AWSElasticBeanstalkServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 13 septembre 2017, 23:46 UTC
- Heure modifiée : 18 août 2026, 17:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "${aws:PrincipalAccount}"
    }
},
{
    "Sid" : "EBEKSBByoAlbListenerRuleCreate",
    "Effect" : "Allow",
    "Action" : [
        "elasticloadbalancing:CreateRule",
        "elasticloadbalancing:AddTags"
    ],
    "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*"
    ],
    "Condition" : {
        "Null" : {
            "aws:RequestTag/elasticbeanstalk:environment-id" : "false"
        },
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid" : "EBEKSBByoAlbListenerRuleDelete",
    "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" : "EBEKSBByoAlbEC2SecurityGroupEgress",
    "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}"
        }
    }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticBeanstalkWebTier

Description : Fournissez aux instances de votre environnement de serveur Web l'accès pour télécharger des fichiers journaux sur Amazon S3.

AWSElasticBeanstalkWebTier est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticBeanstalkWebTier à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 février 2016, 23:08 UTC
- Heure modifiée : 29 avril 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "AIEEnvironmentAnalysisInvokeFoundationModel",
    "Effect" : "Allow",
    "Action" : "bedrock:InvokeModel",
    "Resource" : [
        "arn:aws:bedrock:*:*:foundation-model/anthropic.claude-*",
        "arn:aws:bedrock:*:*:foundation-model/amazon.nova-*"
    ]
},

```

```

{
  "Sid" : "AIEEnvironmentAnalysisInvokeInferenceProfile",
  "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" : "AIEEnvironmentAnalysisReadOnly",
  "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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticBeanstalkWorkerTier

Description : Fournissez aux instances de votre environnement de travail l'accès pour télécharger des fichiers journaux sur Amazon S3, pour utiliser Amazon SQS pour surveiller la file d'attente des tâches de votre candidature, pour utiliser Amazon DynamoDB pour procéder à l'élection des dirigeants et pour Amazon CloudWatch pour publier des mesures pour le suivi de l'état de santé.

AWSElasticBeanstalkWorkerTier est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticBeanstalkWorkerTier à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 février 2016, 23:12 UTC
- Heure modifiée : 29 avril 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "AIEEnvironmentAnalysisInvokeFoundationModel",
    "Effect" : "Allow",
    "Action" : "bedrock:InvokeModel",
    "Resource" : [
        "arn:aws:bedrock:*:*:foundation-model/anthropic.claude-*",
        "arn:aws:bedrock:*:*:foundation-model/amazon.nova-*"
    ]
},

```

```

{
  "Sid" : "AIEEnvironmentAnalysisInvokeInferenceProfile",
  "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" : "AIEEnvironmentAnalysisReadOnly",
  "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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticDisasterRecoveryAgentInstallationPolicy

Description : Cette politique permet d'installer l'agent de AWS réplication, qui est utilisé avec AWS Elastic Disaster Recovery (DRS) pour restaurer des serveurs externes AWS. Attachez cette politique à vos utilisateurs ou rôles IAM dont vous fournissez les informations d'identification lors de l'étape d'installation de l'agent de AWS réplication.

AWSElasticDisasterRecoveryAgentInstallationPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticDisasterRecoveryAgentInstallationPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 novembre 2021, 10:37 UTC
- Heure modifiée : 27 novembre 2023, 12:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryAgentInstallationPolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticDisasterRecoveryAgentPolicy

Description : Cette politique permet d'utiliser l'agent de AWS réplication, qui est utilisé avec AWS Elastic Disaster Recovery (DRS) pour restaurer les serveurs sources AWS. Nous vous déconseillons d'associer cette politique à vos utilisateurs ou rôles IAM.

AWSElasticDisasterRecoveryAgentPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticDisasterRecoveryAgentPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 17 novembre 2021, 10:32 UTC
- Heure modifiée : 27 novembre 2023, 13:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticDisasterRecoveryConsoleFullAccess

Description : Cette politique fournit un accès complet à toutes les API publiques d' AWS Elastic Disaster Recovery (DRS), ainsi que des autorisations pour lire la clé KMS, le gestionnaire de licences, les groupes de ressources, Elastic Load Balancing, IAM et les informations EC2. Associez cette politique à vos utilisateurs ou rôles IAM.

AWSElasticDisasterRecoveryConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticDisasterRecoveryConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 novembre 2021, 10:46 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/
AWS Elastic Disaster Recovery Conversion Server Role",
        "arn:aws:iam::*:role/service-role/
AWS Elastic Disaster Recovery Recovery Instance Role"
    ],
    "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"
      }
    }
  }
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticDisasterRecoveryConsoleFullAccess_v2

Description : Cette politique fournit un accès complet à toutes les API publiques d' AWS Elastic Disaster Recovery (AWS DRS), ainsi qu'à toutes les API publiques AWS des autres services utilisés par AWS DRS Console. Associez cette politique à vos utilisateurs ou à vos rôles.

AWSElasticDisasterRecoveryConsoleFullAccess_v2 est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticDisasterRecoveryConsoleFullAccess_v2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 novembre 2023, 13:35 UTC
- Heure modifiée : 18 juin 2026, 22:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess_v2`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/
AWS Elastic Disaster Recovery Conversion Server Role",
        "arn:aws:iam::*:role/service-role/
AWS Elastic Disaster Recovery Recovery Instance Role",
        "arn:aws:iam::*:role/service-role/
AWS Elastic Disaster Recovery Recovery Instance With Launch Actions Role"
    ]
}

```

```
    ],
    "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"
      }
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticDisasterRecoveryConversionServerPolicy

Description : Cette politique est associée au rôle d'instance du serveur AWS Elastic Disaster Recovery Conversion. Cette politique permet aux serveurs de conversion Elastic Disaster Recovery (DRS), qui sont des instances EC2 lancées par Elastic Disaster Recovery, de communiquer avec le service DRS. Un rôle IAM avec cette politique est attaché (en tant que profil d'instance EC2) par DRS aux serveurs de conversion DRS, qui sont automatiquement lancés et interrompus par DRS, en cas de besoin. Nous vous déconseillons d'associer cette politique à vos utilisateurs ou

rôles IAM. Les serveurs de conversion DRS sont utilisés par Elastic Disaster Recovery lorsque les utilisateurs choisissent de restaurer les serveurs sources à l'aide de la console, de l'interface de ligne de commande ou de l'API DRS.

AWSElasticDisasterRecoveryConversionServerPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticDisasterRecoveryConversionServerPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 17 novembre 2021, 13:42 UTC
- Heure modifiée : 27 novembre 2023, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryConversionServerPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

Description : Cette politique permet à AWS Elastic Disaster Recovery (DRS) de prendre en charge la réplication entre comptes et le failback entre comptes.

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticDisasterRecoveryCrossAccountReplicationPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 14 mai 2023, 07:16 UTC

- Heure modifiée : 17 janvier 2024, 13:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryCrossAccountReplicationPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

```
}  
  }  
] }  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticDisasterRecoveryEc2InstancePolicy

Description : Cette politique autorise l'installation et l'utilisation de l'agent de AWS réplication, qui est utilisé par AWS Elastic Disaster Recovery (DRS) pour restaurer les serveurs sources qui s'exécutent sur EC2 (inter-régions ou cross-AZ). Un rôle IAM avec cette politique doit être attaché (en tant que profil d'instance EC2) aux instances EC2.

AWSElasticDisasterRecoveryEc2InstancePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticDisasterRecoveryEc2InstancePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 26 mai 2022, 12:30 UTC
- Heure modifiée : 27 novembre 2023, 13:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticDisasterRecoveryFailbackInstallationPolicy

Description : Vous pouvez associer la `AWSElasticDisasterRecoveryFailbackInstallationPolicy` politique à vos identités IAM. Cette politique permet d'installer le client Elastic Disaster Recovery Failback, qui est utilisé pour restaurer les instances de restauration sur votre infrastructure source d'origine. Associez cette politique à vos utilisateurs ou rôles IAM dont vous fournissez les informations d'identification lors de l'exécution du client Elastic Disaster Recovery Failback.

`AWSElasticDisasterRecoveryFailbackInstallationPolicy` est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSElasticDisasterRecoveryFailbackInstallationPolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 novembre 2021, 11:02 UTC
- Heure modifiée : 27 novembre 2023, 13:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryFailbackInstallationPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticDisasterRecoveryFailbackPolicy

Description : Cette politique permet d'utiliser le client Elastic Disaster Recovery Failback, qui est utilisé pour restaurer les instances de restauration sur votre infrastructure source d'origine. Nous vous déconseillons d'associer cette politique à vos utilisateurs ou rôles IAM.

AWSElasticDisasterRecoveryFailbackPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticDisasterRecoveryFailbackPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- **Type** : Politique relative aux rôles de service
- **Heure de création** : 17 novembre 2021, 10:41 UTC
- **Heure modifiée** : 22 juillet 2026, 18:42 UTC
- **ARN**: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticDisasterRecoveryLaunchActionsPolicy

Description : Cette politique vous permet d'utiliser Amazon SSM et les autorisations requises pour les services supplémentaires pour exécuter des actions après le lancement dans AWS Elastic Disaster Recovery (AWS DRS). Associez cette politique à vos rôles ou utilisateurs IAM.

AWSElasticDisasterRecoveryLaunchActionsPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticDisasterRecoveryLaunchActionsPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 septembre 2023, 07:38 UTC
- Heure modifiée : 18 juin 2026, 22:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryLaunchActionsPolicy`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/AWSDistro0Tel-*",
    "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/AWSDistro0Tel-*:*",
"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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticDisasterRecoveryNetworkReplicationPolicy

Description : Cette politique permet à AWS Elastic Disaster Recovery (DRS) de prendre en charge la réplication du réseau.

AWSElasticDisasterRecoveryNetworkReplicationPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticDisasterRecoveryNetworkReplicationPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 11 juin 2023, 12:36 UTC
- Heure modifiée : 02 janvier 2024, 13:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryNetworkReplicationPolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticDisasterRecoveryReadOnlyAccess

Description : Vous pouvez associer la AWSElasticDisasterRecoveryReadOnlyAccess politique à vos identités IAM. Cette politique fournit des autorisations à toutes les API publiques en lecture

seule d'Elastic Disaster Recovery (DRS), ainsi qu'à certaines API en lecture seule d'autres AWS services qui sont nécessaires pour utiliser pleinement la console DRS en lecture seule. Associez cette politique à vos utilisateurs ou rôles IAM.

AWSElasticDisasterRecoveryReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticDisasterRecoveryReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 novembre 2021, 10:50 UTC
- Heure modifiée : 18 août 2026, 14:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
}

```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticDisasterRecoveryRecoveryInstancePolicy

Description : Cette politique est associée au rôle d'instance de l'instance de restauration d'Elastic Disaster Recovery. Cette politique permet à l'instance Elastic Disaster Recovery (DRS) Recovery, qui sont des instances EC2 lancées par Elastic Disaster Recovery, de communiquer avec le service DRS et de revenir à leur infrastructure source d'origine. Un rôle IAM avec cette politique est attaché (en tant que profil d'instance EC2) par Elastic Disaster Recovery aux instances DRS Recovery. Nous vous recommandons d'associer cette politique à vos utilisateurs ou rôles IAM.

AWSElasticDisasterRecoveryRecoveryInstancePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticDisasterRecoveryRecoveryInstancePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 17 novembre 2021, 10:20 UTC
- Heure modifiée : 27 novembre 2023, 13:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryRecoveryInstancePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticDisasterRecoveryReplicationServerPolicy

Description : Cette politique est associée au rôle d'instance du serveur Elastic Disaster Recovery Replication. Cette politique permet aux serveurs de réplication Elastic Disaster Recovery (DRS), qui sont des instances EC2 lancées par Elastic Disaster Recovery, de communiquer avec le service DRS et de créer des instantanés EBS dans votre. Compte AWS Un rôle IAM avec cette politique est attaché (en tant que profil d'instance EC2) par Elastic Disaster Recovery aux serveurs de réplication DRS qui sont automatiquement lancés et interrompus par DRS, selon les besoins. Les serveurs de

réplication DRS sont utilisés pour faciliter la réplication des données depuis vos serveurs externes vers AWS, dans le cadre du processus de restauration géré par DRS. Nous vous déconseillons d'associer cette politique à vos utilisateurs ou rôles IAM.

`AWSElasticDisasterRecoveryReplicationServerPolicy` est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSElasticDisasterRecoveryReplicationServerPolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 17 novembre 2021, 13:34 UTC
- Heure modifiée : 27 novembre 2023, 13:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticDisasterRecoveryServiceRolePolicy

Description : Cette politique permet à Elastic Disaster Recovery de gérer les AWS ressources en votre nom.

AWSElasticDisasterRecoveryServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 17 novembre 2021, 10:56 UTC
- Heure modifiée : 05 janvier 2025, 14:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticDisasterRecoveryServiceRolePolicy`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticDisasterRecoveryStagingAccountPolicy

Description : Cette politique autorise l'accès en lecture seule aux ressources AWS Elastic Disaster Recovery (DRS) telles que les serveurs sources et les tâches. Il permet également de créer un instantané converti et de partager cet instantané EBS avec un compte spécifique.

AWSElasticDisasterRecoveryStagingAccountPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSElasticDisasterRecoveryStagingAccountPolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 26 mai 2022, 09:49 UTC
- Heure modifiée : 27 novembre 2023, 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

Description : Cette politique est utilisée par AWS Elastic Disaster Recovery (DRS) pour restaurer les serveurs sources sur un compte cible distinct et pour autoriser le retour en arrière. Nous vous déconseillons d'associer cette politique à vos utilisateurs ou rôles IAM.

AWSElasticDisasterRecoveryStagingAccountPolicy_v2 est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElasticDisasterRecoveryStagingAccountPolicy_v2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 05 janvier 2023, 12:11 UTC
- Heure modifiée : 09 septembre 2026, 13:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticLoadBalancingClassicServiceRolePolicy

Description : Politique de rôle lié aux services pour AWS Elastic Load Balancing Control Plane - Classic

AWSElasticLoadBalancingClassicServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 19 septembre 2017, 22:36 UTC
- Heure modifiée : 07 octobre 2019, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElasticLoadBalancingServiceRolePolicy

Description : Politique de rôle lié aux services pour AWS Elastic Load Balancing Control Plane

AWSElasticLoadBalancingServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 19 septembre 2017, 22:19 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy`

Version de la politique

Version de la politique : v14 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElementalMediaConnectCreateBridge

Description : fournit un accès complet pour créer des MediaConnect passerelles et toutes les sous-ressources associées.

AWSElementalMediaConnectCreateBridge est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSElementalMediaConnectCreateBridge` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 mars 2026, 16:57 UTC
- Heure modifiée : 19 mars 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectCreateBridge`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
      ]
    }
  ]
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElementalMediaConnectCreateFlow

Description : fournit un accès complet à la création de MediaConnect flux et à toutes les sous-ressources associées.

AWSElementalMediaConnectCreateFlowest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElementalMediaConnectCreateFlow à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 mars 2026, 16:57 UTC
- Heure modifiée : 19 mars 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectCreateFlow`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "mediacconnect.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mediacconnect:CreateFlow",
        "mediacconnect:AddFlowSources",
        "mediacconnect:AddFlowOutputs",
        "mediacconnect:GrantFlowEntitlements",
        "mediacconnect:AddFlowMediaStreams",
        "mediacconnect:AddFlowVpcInterfaces",
        "mediacconnect:TagResource"
      ],
      "Resource" : [
        "arn:aws:mediacconnect::*:flow:*:*",
        "arn:aws:mediacconnect::*:source:*:*",
        "arn:aws:mediacconnect::*:output:*:*",
        "arn:aws:mediacconnect::*:entitlement:*:*",
        "arn:aws:mediacconnect::*:flow:*:*/vpcInterface/*",
        "arn:aws:mediacconnect::*:flow:*:*/mediaStream/*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElementalMediaConnectDeleteBridge

Description : fournit un accès complet pour supprimer MediaConnect Gateway Bridges et toutes ses sous-ressources associées.

AWSElementalMediaConnectDeleteBridge est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElementalMediaConnectDeleteBridge à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 mars 2026, 19:57 UTC
- Heure modifiée : 19 mars 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectDeleteBridge`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElementalMediaConnectDeleteFlow

Description : fournit un accès complet pour supprimer MediaConnect Flows et toutes les sous-ressources associées.

AWSElementalMediaConnectDeleteFlowest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElementalMediaConnectDeleteFlow à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 mars 2026, 19:57 UTC

- Heure modifiée : 19 mars 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectDeleteFlow`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElementalMediaConnectFullAccess

Description : Fournit un accès complet aux MediaConnect ressources AWS élémentaires.

AWSElementalMediaConnectFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElementalMediaConnectFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 février 2025, 20:07 UTC
- Heure modifiée : 12 février 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
    "Action" : [
      "mediacconnect:*"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElementalMediaConnectReadOnlyAccess

Description : fournit un accès en lecture seule aux ressources AWS élémentaires MediaConnect .

AWSElementalMediaConnectReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElementalMediaConnectReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 février 2025, 20:07 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElementalMediaConvertFullAccess

Description : fournit un accès complet à AWS Elemental MediaConvert via le SDK Console de gestion AWS et.

AWSElementalMediaConvertFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElementalMediaConvertFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 juin 2018, 19:25 UTC
- Heure modifiée : 10 juin 2019, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElementalMediaConvertReadOnly

Description : fournit un accès en lecture seule à AWS Elemental MediaConvert via le SDK Console de gestion AWS et.

AWSElementalMediaConvertReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElementalMediaConvertReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 25 juin 2018, 19:25 UTC
- Heure modifiée : 10 juin 2019, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "mediaconvert:DescribeEndpoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElementalMediaLiveFullAccess

Description : Fournit un accès complet aux AWS ressources élémentaires MediaLive

AWSElementalMediaLiveFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElementalMediaLiveFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 juillet 2020, 17:07 UTC
- Heure modifiée : 08 juillet 2020, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElementalMediaLiveReadOnly

Description : fournit un accès en lecture seule aux AWS ressources élémentaires MediaLive

AWSElementalMediaLiveReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElementalMediaLiveReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 juillet 2020, 16:38 UTC
- Heure modifiée : 22 juillet 2024, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
        "medialive:Get*",
        "medialive:List*",
        "medialive:Describe"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElementalMediaPackageFullAccess

Description : Fournit un accès complet aux AWS ressources élémentaires MediaPackage

AWSElementalMediaPackageFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElementalMediaPackageFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 décembre 2017, 23:39 UTC
- Heure modifiée : 29 décembre 2017, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElementalMediaPackageReadOnly

Description : fournit un accès en lecture seule aux AWS ressources élémentaires MediaPackage

AWSElementalMediaPackageReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElementalMediaPackageReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 décembre 2017, 00:04 UTC
- Heure modifiée : 30 décembre 2017, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElementalMediaPackageV2FullAccess

Description : fournit un accès complet aux ressources d' AWS Elemental MediaPackage V2.

AWSElementalMediaPackageV2FullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElementalMediaPackageV2FullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 juillet 2023, 20:29 UTC
- Heure modifiée : 25 juillet 2023, 20:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElementalMediaPackageV2ReadOnly

Description : fournit un accès en lecture seule aux ressources d' AWS Elemental V2. MediaPackage

AWSElementalMediaPackageV2ReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElementalMediaPackageV2ReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 juillet 2023, 20:31 UTC
- Heure modifiée : 25 juillet 2023, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackagev2:List*",
      "mediapackagev2:Get*"
    ],
    "Resource" : "*"
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElementalMediaStoreFullAccess

Description : fournit un accès complet en lecture et en écriture à toutes les MediaStore API

AWSElementalMediaStoreFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElementalMediaStoreFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 mars 2018, 23:15 UTC
- Heure modifiée : 05 mars 2018, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:*"
      ],

```

```
"Effect" : "Allow",
"Resource" : "*",
"Condition" : {
  "Bool" : {
    "aws:SecureTransport" : "true"
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElementalMediaStoreReadOnly

Description : fournit des autorisations en lecture seule pour les API MediaStore

AWSElementalMediaStoreReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElementalMediaStoreReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 mars 2018, 19:48 UTC
- Heure modifiée : 08 mars 2018, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:Get*",
        "mediastore:List*",
        "mediastore:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElementalMediaTailorFullAccess

Description : Fournit un accès complet aux AWS ressources élémentaires MediaTailor

AWSElementalMediaTailorFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSElementalMediaTailorFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 novembre 2021, 00:04 UTC
- Heure modifiée : 23 novembre 2021, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSElementalMediaTailorReadOnly

Description : fournit un accès en lecture seule aux AWS ressources élémentaires MediaTailor

AWSElementalMediaTailorReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSElementalMediaTailorReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 novembre 2021, 00:05 UTC
- Heure modifiée : 23 novembre 2021, 00:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSEnhancedClassicNetworkingMangementPolicy

Description : Politique visant à activer la fonctionnalité de gestion réseau classique améliorée.

AWSEnhancedClassicNetworkingMangementPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 20 septembre 2017, 17:29 UTC
- Heure modifiée : 20 septembre 2017, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSEntityResolutionConsoleFullAccess

Description : fournit à la console un accès complet à AWS Entity Resolution et aux services associés.

AWSEntityResolutionConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSEntityResolutionConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 août 2023, 17:54 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSEntityResolutionConsoleReadOnlyAccess

Description : fournit un accès en lecture seule à AWS Entity Resolution via le. Console de gestion AWS

AWSEntityResolutionConsoleReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSEntityResolutionConsoleReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 août 2023, 18:18 UTC
- Heure modifiée : 17 août 2023, 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSFaultInjectionSimulatorEC2Access

Description : Cette politique accorde l'autorisation au service Fault Injection Simulator dans EC2 et aux autres services requis pour effectuer des actions FIS.

AWSFaultInjectionSimulatorEC2Access est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSFaultInjectionSimulatorEC2Access` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 26 octobre 2022, 20:39 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSFaultInjectionSimulatorECSAccess

Description : Cette politique accorde au service Fault Injection Simulator l'autorisation d'exécuter des actions FIS dans ECS et dans d'autres services requis.

AWSFaultInjectionSimulatorECSAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSFaultInjectionSimulatorECSAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 26 octobre 2022, 20:37 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSFaultInjectionSimulatorEKSAccess

Description : Cette politique accorde au service Fault Injection Simulator l'autorisation d'effectuer des actions FIS dans EKS et d'autres services requis.

AWSFaultInjectionSimulatorEKSAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSFaultInjectionSimulatorEKSAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 26 octobre 2022, 20:34 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSFaultInjectionSimulatorNetworkAccess

Description : Cette politique accorde au service Fault Injection Simulator l'autorisation d'accéder au réseau EC2 et aux autres services requis pour effectuer des actions FIS.

AWSFaultInjectionSimulatorNetworkAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSFaultInjectionSimulatorNetworkAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 26 octobre 2022, 20:32 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
  }
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSFaultInjectionSimulatorRDSAccess

Description : Cette politique accorde au service Fault Injection Simulator l'autorisation d'utiliser RDS et d'autres services requis pour effectuer des actions FIS.

AWSFaultInjectionSimulatorRDSAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSFaultInjectionSimulatorRDSAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 26 octobre 2022, 20:30 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSFaultInjectionSimulatorSSMAccess

Description : Cette politique accorde au service Fault Injection Simulator l'autorisation d'utiliser SSM et d'autres services requis pour effectuer des actions FIS.

AWSFaultInjectionSimulatorSSMAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSFaultInjectionSimulatorSSMAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 26 octobre 2022, 15:33 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"   
    }  
  ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSFinSpaceServiceRolePolicy

Description : Politique visant à autoriser l'accès Service AWS aux ressources utilisées ou gérées par Amazon FinSpace

AWSFinSpaceServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 12 mai 2023, 16:42 UTC
- Heure modifiée : 01 décembre 2023, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSFMAdminFullAccess

Description : Accès complet pour AWS FM Administrator

AWSFMAdminFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSFMAdminFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 mai 2018, 18:06 UTC
- Heure modifiée : 20 octobre 2022, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      ]
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSFMAdminReadOnlyAccess

Description : Accès en lecture seule pour AWS FM Administrator qui permet de surveiller les opérations AWS FM

AWSFMAdminReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSFMAdminReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 mai 2018, 20:07 UTC
- Heure modifiée : 31 octobre 2022, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSFMMemberReadOnlyAccess

Description : fournit un accès en lecture seule aux actions AWS WAF pour les comptes membres de AWS Firewall Manager

AWSFMMemberReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSFMMemberReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 mai 2018, 21:05 UTC
- Heure modifiée : 09 mai 2018, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSForWordPressPluginPolicy

Description : Politique gérée pour le plugin AWS For Wordpress

AWSForWordPressPluginPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSForWordPressPluginPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 octobre 2019, 00:27 UTC
- Heure modifiée : 03 septembre 2026, 20:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSGitSyncServiceRolePolicy

Description : Politique qui permet à AWS Code Connections de synchroniser le contenu de votre référentiel git

AWSGitSyncServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 16 novembre 2023, 17:05 UTC
- Heure modifiée : 26 avril 2024, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
      }
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSGlobalAcceleratorSLRPolicy

Description : Politique accordant des autorisations à AWS Global Accelerator pour gérer les interfaces réseau élastiques et les groupes de sécurité EC2.

AWSGlobalAcceleratorSLRPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 05 avril 2019, 19:39 UTC
- Heure modifiée : 29 octobre 2024, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSGlueConsoleFullAccess

Description : Fournit un accès complet à AWS Glue via Console de gestion AWS

AWSGlueConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSGlueConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 août 2017, 13:37 UTC
- Heure modifiée : 10 septembre 2026, 20:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess

Version de la politique

Version de la politique : v15 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
                ]
            }
        }
    }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSGlueConsoleSageMakerNotebookFullAccess

Description : fournit un accès complet à AWS Glue via les instances de bloc-notes Sagemaker Console de gestion AWS et un accès aux instances de bloc-notes.

AWSGlueConsoleSageMakerNotebookFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSGlueConsoleSageMakerNotebookFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 octobre 2018, 17:52 UTC
- Heure modifiée : 10 septembre 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      ]
    }
  }
}
]
```



```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AwsGlueDataBrewFullAccessPolicy

Description : Fournit un accès complet à AWS Glue DataBrew via le Console de gestion AWS. Fournit également un accès sélectif à des services connexes (par exemple, S3, KMS, Glue).

AwsGlueDataBrewFullAccessPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AwsGlueDataBrewFullAccessPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 novembre 2020, 16:51 UTC
- Heure modifiée : 04 février 2022, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSGlueDataBrewServiceRole

Description : Cette politique autorise Glue à effectuer une action sur le catalogue de données Glue de l'utilisateur. Cette politique autorise également les actions ec2 pour autoriser Glue à créer une ENI pour se connecter aux ressources du VPC, autoriser Glue à accéder aux données enregistrées dans Lakeformation et autoriser Glue à accéder aux données enregistrées dans Lakeformation et l'autorisation d'accéder à la Cloudwatch de l'utilisateur

AWSGlueDataBrewServiceRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSGlueDataBrewServiceRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 04 décembre 2020, 21:26 UTC
- Heure modifiée : 20 mars 2024, 23:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSGlueSchemaRegistryFullAccess

Description : fournit un accès complet au service de registre AWS Glue Schema

AWSGlueSchemaRegistryFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSGlueSchemaRegistryFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 novembre 2020, 00:19 UTC
- Heure modifiée : 20 novembre 2020, 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSGlueSchemaRegistryReadonlyAccess

Description : fournit un accès en lecture seule au service de registre AWS Glue Schema

AWSGlueSchemaRegistryReadonlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSGlueSchemaRegistryReadonlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 novembre 2020, 00:20 UTC
- Heure modifiée : 20 novembre 2020, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadonlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
    "*"
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSGlueServiceNotebookRole

Description : Politique relative au rôle de service AWS Glue qui permet au client de gérer le serveur de blocs-notes

AWSGlueServiceNotebookRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSGlueServiceNotebookRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 14 août 2017, 13:37 UTC
- Heure modifiée : 09 octobre 2023, 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSGlueServiceRole

Description : Politique pour le rôle de service AWS Glue qui permet d'accéder aux services associés, notamment EC2, S3 et Cloudwatch Logs

AWSGlueServiceRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSGlueServiceRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 14 août 2017, 13:37 UTC
- Heure modifiée : 11 septembre 2023, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AwsGlueSessionUserRestrictedNotebookPolicy

Description : fournit des autorisations qui permettent aux utilisateurs de créer et d'utiliser uniquement les sessions de bloc-notes qui leur sont associées. Cette politique inclut également des autorisations permettant explicitement aux utilisateurs de transmettre un rôle de session Glue restreint.

AwsGlueSessionUserRestrictedNotebookPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AwsGlueSessionUserRestrictedNotebookPolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 avril 2022, 15:24 UTC
- Heure modifiée : 15 août 2024, 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      ]
    }
  }
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AwsGlueSessionUserRestrictedNotebookServiceRole

Description : fournit un accès complet à toutes les ressources de AWS Glue, à l'exception des sessions. Permet aux utilisateurs de créer et d'utiliser uniquement les séances de bloc-notes associées à l'utilisateur. Cette politique inclut également d'autres autorisations nécessaires à AWS Glue pour gérer les ressources Glue dans d'autres AWS services.

AwsGlueSessionUserRestrictedNotebookServiceRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AwsGlueSessionUserRestrictedNotebookServiceRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service

- Heure de création : 18 avril 2022, 15:27 UTC
- Heure modifiée : 15 août 2024, 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AwsGlueSessionUserRestrictedPolicy

Description : fournit des autorisations qui permettent aux utilisateurs de créer et d'utiliser uniquement les sessions interactives qui leur sont associées. Cette politique inclut également des autorisations permettant explicitement aux utilisateurs de transmettre un rôle de session Glue restreint.

AwsGlueSessionUserRestrictedPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AwsGlueSessionUserRestrictedPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 avril 2022, 21:31 UTC
- Heure modifiée : 05 août 2024, 23:06 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSessionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:user}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:user}"
        }
      }
    }
  ]
}
```

```
        "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"
        ]
      }
    }
  }
]
```


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AwsGlueSessionUserRestrictedServiceRole

Description : fournit un accès complet à toutes les ressources de AWS Glue, à l'exception des sessions. Permet aux utilisateurs de créer et d'utiliser uniquement les séances interactives associées à l'utilisateur. Cette politique inclut également d'autres autorisations nécessaires à AWS Glue pour gérer les ressources Glue dans d'autres AWS services.

AwsGlueSessionUserRestrictedServiceRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AwsGlueSessionUserRestrictedServiceRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 14 avril 2022, 21:30 UTC
- Heure modifiée : 05 août 2024, 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSGrafanaAccountAdministrator

Description : permet d'accéder à Amazon Grafana pour créer et gérer des espaces de travail pour l'ensemble de l'organisation.

AWSGrafanaAccountAdministrator est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSGrafanaAccountAdministrator à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 février 2021, 00:20 UTC
- Heure modifiée : 15 février 2022, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

```
}  
  }  
    }  
      ]  
    }  
  }
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSGrafanaConsoleReadOnlyAccess

Description : Accès aux opérations en lecture seule dans Amazon Grafana.

AWSGrafanaConsoleReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSGrafanaConsoleReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 février 2021, 00:10 UTC
- Heure modifiée : 15 février 2022, 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaConsoleReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:Describe*",
        "grafana:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSGrafanaWorkspacePermissionManagement

Description : permet uniquement de mettre à jour les autorisations des utilisateurs et des groupes pour les espaces de travail AWS Grafana.

AWSGrafanaWorkspacePermissionManagement est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSGrafanaWorkspacePermissionManagement à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 23 février 2021, 00:15 UTC
- Heure modifiée : 15 mars 2023, 22:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSGrafanaWorkspacePermissionManagementV2

Description : permet de mettre à jour les autorisations des utilisateurs et des groupes IAM Identity Center (iDC) pour les espaces de travail Amazon Managed Grafana.

AWSGrafanaWorkspacePermissionManagementV2 est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSGrafanaWorkspacePermissionManagementV2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 janvier 2024, 18:39 UTC
- Heure modifiée : 05 janvier 2024, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSGreengrassFullAccess

Description : Cette politique donne un accès complet aux actions de configuration, de gestion et de déploiement de AWS Greengrass

AWSGreengrassFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSGreengrassFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 mai 2017, 00:47 UTC
- Heure modifiée : 03 mai 2017, 00:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSGreengrassReadOnlyAccess

Description : Cette politique donne un accès en lecture seule aux actions de configuration, de gestion et de déploiement de AWS Greengrass

AWSGreengrassReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSGreengrassReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 octobre 2018, 16:01 UTC
- Heure modifiée : 30 octobre 2018, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSGreengrassResourceAccessRolePolicy

Description : Politique pour le rôle de service AWS Greengrass qui permet d'accéder à des services connexes, notamment AWS Lambda et AWS IoT Thing Shadows.

AWSGreengrassResourceAccessRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSGreengrassResourceAccessRolePolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 14 février 2017, 21:17 UTC
- Heure modifiée : 14 novembre 2018, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSGroundStationAgentInstancePolicy

Description : fournit à l'instance de point de terminaison de flux de données les autorisations nécessaires pour utiliser l'agent AWS Ground Station

AWSGroundStationAgentInstancePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSGroundStationAgentInstancePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 mars 2023, 15:23 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "groundstation:RegisterAgent",
        "groundstation:UpdateAgentStatus",
        "groundstation:GetAgentConfiguration",
```

```
        "groundstation:GetAgentTaskResponseUrl"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWS Health_EventProcessorServiceRolePolicy

Description : permet à AWS Health d'activer la fonction de traitement des événements de santé.

AWSHealth_EventProcessorServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 13 janvier 2023, 19:24 UTC
- Heure modifiée : 13 janvier 2023, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealth_EventProcessorServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSHealthFullAccess

Description : Permet un accès complet aux API et notifications de AWS santé et au tableau de bord de santé personnel

AWSHealthFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSHealthFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 décembre 2016, 12:30 UTC
- Heure modifiée : 16 novembre 2020, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSHealthImagingFullAccess

Description : Fournit un accès complet au service d'imagerie AWS médicale.

AWSHealthImagingFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSHealthImagingFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 juillet 2023, 23:39 UTC
- Heure modifiée : 25 juillet 2023, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```



```
}  
  }  
  ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSHealthImagingReadOnlyAccess

Description : Fournit un accès en lecture seule au service d'imagerie AWS médicale.

AWSHealthImagingReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSHealthImagingReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 juillet 2023, 23:40 UTC
- Heure modifiée : 01 août 2023, 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSHealthImagingServiceRolePolicy

Description : Fournit les autorisations nécessaires AWS HealthImaging pour gérer les opérations de service et publier des mesures de service

AWSHealthImagingServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 30 janvier 2026, 18:34 UTC
- Heure modifiée : 30 janvier 2026, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealthImagingServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSHealthOmicsServiceLinkedRolePolicy

Description : Politique gérée pour le rôle lié à Amazon HealthOmics Service

AWSHealthOmicsServiceLinkedRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 04 mars 2026, 22:57 UTC
- Heure modifiée : 04 mars 2026, 22:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealthOmicsServiceLinkedRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIAMIdentityCenterAllowListForIdentityContext

Description : fournit la liste des actions autorisées pour les rôles assumés dans le contexte d'identité IAM Identity Center. AWS Le Security Token Service (AWS STS) associe automatiquement cette politique aux rôles assumés. Le contexte d'identité est transmis en tant que `ProvidedContext`.

AWSIAMIdentityCenterAllowListForIdentityContext est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIAMIdentityCenterAllowListForIdentityContext à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 novembre 2023, 15:21 UTC
- Heure modifiée : 01 octobre 2024, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIAMIdentityCenterAllowListForIdentityContext`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:ListPreparedStatement",
"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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIAMRoleManagerServiceRolePolicy

Description : permet à IAM Role Manager de gérer les ressources de votre compte en votre nom.

AWSIAMRoleManagerServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 15 juillet 2026, 23:57 UTC
- Heure modifiée : 05 août 2026, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIAMRoleManagerServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIdentityCenterExternalManagementPolicy

Description : permet de gérer les utilisateurs d'IAM Identity Center depuis un fournisseur externe.

AWSIdentityCenterExternalManagementPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIdentityCenterExternalManagementPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 22 novembre 2025, 00:34 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIdentityCenterExternalManagementPolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIdentitySyncFullAccess

Description : accorde un accès complet au service Identity Sync

AWSIdentitySyncFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIdentitySyncFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 mars 2022, 23:29 UTC
- Heure modifiée : 23 mars 2022, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*:*:*/*/*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIdentitySyncReadOnlyAccess

Description : Accès en lecture seule au service Identity Sync

AWSIdentitySyncReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIdentitySyncReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 mars 2022, 23:29 UTC
- Heure modifiée : 23 mars 2022, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:GetSyncProfile",
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ],
      "Resource" : "arn::*:identity-sync:*:*:*/*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSImageBuilderFullAccess

Description : fournit un accès complet à toutes les actions AWS d'Image Builder et un accès limité aux ressources aux AWS services associés.

AWSImageBuilderFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSImageBuilderFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 décembre 2019, 18:25 UTC
- Heure modifiée : 13 avril 2021, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSImageBuilderReadOnlyAccess

Description : fournit un accès en lecture seule à toutes les actions AWS d'Image Builder.

AWSImageBuilderReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSImageBuilderReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 décembre 2019, 22:29 UTC
- Heure modifiée : 19 décembre 2019, 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSImportExportFullAccess

Description : Fournit un accès en lecture et en écriture aux tâches créées dans le cadre du Compte AWS.

AWSImportExportFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSImportExportFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 06 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSImportExportReadOnlyAccess

Description : fournit un accès en lecture seule aux emplois créés dans le cadre du Compte AWS.

AWSImportExportReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSImportExportReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 06 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
```



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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIncidentManagerIncidentAccessServiceRolePolicy

Description : accorde au gestionnaire d'incidents les autorisations nécessaires pour appeler d'autres AWS services dans le cadre de la gestion d'un incident.

AWSIncidentManagerIncidentAccessServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIncidentManagerIncidentAccessServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 novembre 2023, 00:01 UTC
- Heure modifiée : 20 février 2024, 23:02 UTC

- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerIncidentAccessServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IncidentAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIncidentManagerResolverAccess

Description : Cette politique accorde des autorisations pour démarrer, afficher et mettre à jour des incidents avec un accès complet aux événements chronologiques personnalisés et aux éléments associés. Attribuez cette politique aux utilisateurs qui créeront et résoudront les incidents.

AWSIncidentManagerResolverAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIncidentManagerResolverAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 10 mai 2021, 06:12 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIncidentManagerServiceRolePolicy

Description : Cette politique accorde à Incident Manager l'autorisation de gérer les dossiers d'incidents et les ressources associées en votre nom.

AWSIncidentManagerServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 10 mai 2021, 03:34 UTC
- Heure modifiée : 28 janvier 2025, 02:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            ]
        }
    }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoT1ClickFullAccess

Description : fournit un accès complet à AWS IoT 1-Click.

AWSIoT1ClickFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoT1ClickFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 mai 2018, 22:10 UTC
- Heure modifiée : 11 mai 2018, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoT1ClickReadOnlyAccess

Description : fournit un accès en lecture seule à AWS IoT 1-Click.

AWSIoT1ClickReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoT1ClickReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 mai 2018, 21:49 UTC
- Heure modifiée : 11 mai 2018, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "iot1click:Describe*",
      "iot1click:Get*",
      "iot1click:List*"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTAnalyticsFullAccess

Description : fournit un accès complet à IoT Analytics.

AWSIoTAnalyticsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTAnalyticsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 juin 2018, 23:02 UTC
- Heure modifiée : 18 juin 2018, 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTAnalyticsReadOnlyAccess

Description : fournit un accès en lecture seule à IoT Analytics.

AWSIoTAnalyticsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTAnalyticsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 juin 2018, 21:37 UTC
- Heure modifiée : 18 juin 2018, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTConfigAccess

Description : Cette politique donne un accès complet aux actions de configuration AWS IoT

AWSIoTConfigAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTConfigAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 octobre 2015, 21:52 UTC
- Heure modifiée : 27 septembre 2019, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigAccess`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTConfigReadOnlyAccess

Description : Cette politique donne un accès en lecture seule aux actions de configuration AWS IoT

AWSIoTConfigReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTConfigReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 octobre 2015, 21:52 UTC
- Heure modifiée : 27 septembre 2019, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTDataAccess

Description : Cette politique donne un accès complet aux actions de messagerie AWS IoT

AWSIoTDataAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTDataAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 octobre 2015, 21:51 UTC
- Heure modifiée : 23 juin 2021, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDataAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

Description : fournit un accès en écriture aux groupes d'objets IoT et un accès en lecture aux certificats IoT pour l'exécution de l'action d'atténuation ADD_THINGS_TO_THING_GROUP

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 07 août 2019, 17:55 UTC
- Heure modifiée : 07 août 2019, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
    "iot:AddThingToThingGroup"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTDeviceDefenderAudit

Description : fournit un accès en lecture pour l'IoT et les ressources associées

AWSIoTDeviceDefenderAudit est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTDeviceDefenderAudit à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 18 juillet 2018, 21:17 UTC
- Heure modifiée : 25 novembre 2019, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

Description : fournit un accès permettant d'activer la journalisation IoT pour l'exécution de l'action d'atténuation ENABLE_IOT_LOGGING

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 07 août 2019, 17:04 UTC
- Heure modifiée : 07 août 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
          ]
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

Description : permet de publier des messages et d'accéder à la rubrique SNS pour l'exécution de l'action d'atténuation PUBLISH_FINDING_TO_SNS

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 07 août 2019, 17:04 UTC
- Heure modifiée : 07 août 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

Description : fournit un accès en écriture aux politiques IoT pour l'exécution de l'action d'atténuation REPLACE_DEFAULT_POLICY_VERSION

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 07 août 2019, 17:04 UTC
- Heure modifiée : 07 août 2019, 17:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTDeviceDefenderUpdateCACertMitigationAction

Description : fournit un accès en écriture aux certificats IoT CA pour l'exécution de l'action d'atténuation UPDATE_CA_CERTIFICATE

AWSIoTDeviceDefenderUpdateCACertMitigationAction est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSIoTDeviceDefenderUpdateCACertMitigationAction` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 07 août 2019, 17:05 UTC
- Heure modifiée : 07 août 2019, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

Description : fournit un accès en écriture aux certificats IoT pour l'exécution de l'action d'atténuation UPDATE_DEVICE_CERTIFICATE

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 07 août 2019, 17:06 UTC
- Heure modifiée : 07 août 2019, 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTDeviceTesterForFreeRTOSFullAccess

Description : permet à AWS IoT Device Tester d'exécuter la suite de qualification FreeRTOS en autorisant l'accès à des services tels que l'IoT, S3 et IAM

AWSIoTDeviceTesterForFreeRTOSFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTDeviceTesterForFreeRTOSFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 12 février 2020, 20:33 UTC
- Heure modifiée : 10 août 2023, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTDeviceTesterForGreengrassFullAccess

Description : Permet à AWS IoT Device Tester d'exécuter la suite de qualification AWS Greengrass en autorisant l'accès aux services associés, notamment Lambda, IoT, API Gateway et IAM

AWSIoTDeviceTesterForGreengrassFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTDeviceTesterForGreengrassFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 20 février 2020, 21:21 UTC
- Heure modifiée : 25 juin 2020, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTEventsFullAccess

Description : fournit un accès complet aux événements IoT.

AWSIoTEventsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTEventsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 10 janvier 2019, 22:51 UTC
- Heure modifiée : 10 janvier 2019, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTEventsReadOnlyAccess

Description : fournit un accès en lecture seule aux événements IoT.

AWSIoTEventsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTEventsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 10 janvier 2019, 22:50 UTC
- Heure modifiée : 23 septembre 2019, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoT FleetHubFederationAccess

Description : Accès fédéré pour les applications IoT Fleet Hub

AWSIoT FleetHubFederationAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoT FleetHubFederationAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 15 décembre 2020, 08:08 UTC
- Heure modifiée : 04 avril 2022, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoT FleetHubFederationAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoT Fleetwise Service Role Policy

Description : accorde des autorisations aux AWS ressources et aux métadonnées utilisées ou gérées par AWSIoT Fleetwise pour les fonctionnalités auxiliaires

AWSIoT Fleetwise Service Role Policy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 21 septembre 2022, 23:27 UTC
- Heure modifiée : 16 octobre 2025, 04:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoT Fleetwise Service Role Policy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTFullAccess

Description : Cette politique donne un accès complet à la configuration de l' AWS IoT et aux actions de messagerie

AWSIoTFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSIoTFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 octobre 2015, 15:19 UTC
- Heure modifiée : 19 mai 2022, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTLogging

Description : Permet la création de groupes Amazon CloudWatch Log et la diffusion de journaux vers les groupes

AWSIoTLoggingest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTLogging à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 08 octobre 2015, 15:17 UTC
- Heure modifiée : 08 octobre 2015, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTLogging`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy",
        "logs:GetLogEvents",
        "logs>DeleteLogStream"
    ],
    "Resource" : [
        "*"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTManagedIntegrationsFullAccess

Description : fournit un accès complet aux intégrations gérées pour la gestion des appareils AWS IoT et les services associés.

AWSIoTManagedIntegrationsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTManagedIntegrationsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 mars 2025, 19:22 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC

- ARN: `arn:aws:iam::aws:policy/AWSIoTManagedIntegrationsFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTManagedIntegrationsRolePolicy

Description : fournit des intégrations gérées pour permettre à la gestion des appareils AWS IoT de publier des journaux et des mesures en votre nom.

AWSIoTManagedIntegrationsRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 05 mars 2025, 21:22 UTC
- Heure modifiée : 05 mars 2025, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTManagedIntegrationsRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      ]
    }
  }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTOTAUpdate

Description : Permet d'accéder à la création d'une tâche AWS IoT et à la description de la tâche du signataire de AWS code

AWSIoTOTAUpdate est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTOTAUpdate à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 20 décembre 2017, 20:36 UTC
- Heure modifiée : 20 décembre 2017, 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTOTAUpdate`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
"Action" : [
  "iot:CreateJob",
  "signer:DescribeSigningJob"
],
"Resource" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTRoboRunnerFullAccess

Description : Cette politique accorde des autorisations qui permettent un accès complet à AWS IoT RoboRunner.

AWSIoTRoboRunnerFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTRoboRunnerFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2021, 03:54 UTC
- Heure modifiée : 23 février 2023, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTRoboRunnerFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTRoboRunnerReadOnly

Description : Cette politique accorde des autorisations qui permettent un accès en lecture seule à AWS IoT. RoboRunner

AWSIoTRoboRunnerReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTRoboRunnerReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2021, 03:43 UTC
- Heure modifiée : 16 novembre 2022, 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTRoboRunnerReadOnly`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTRoboRunnerServiceRolePolicy

Description : Permet RoboRunner à AWS IoT de gérer les AWS ressources associées pour le compte du client.

AWSIoTRoboRunnerServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 21 février 2023, 16:56 UTC
- Heure modifiée : 21 février 2023, 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTRoboRunnerServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTRuleActions

Description : Permet d'accéder à tous les AWS services pris en charge par AWS IoT Rule Actions

AWSIoTRuleAction est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTRuleActions à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 08 octobre 2015, 15:14 UTC

- Heure modifiée : 16 janvier 2018, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTSiteWiseConsoleFullAccess

Description : Fournit un accès complet pour gérer AWS IoT à SiteWise l'aide du Console de gestion AWS. Notez que cette politique donne également accès à la création et à la liste des magasins de données utilisés avec l' AWS IoT SiteWise (par exemple AWS IoT Analytics), à la liste et à l'affichage des ressources AWS IoT Greengrass, à la liste et à la modification des AWS secrets de Secrets Manager, à la récupération des ombres d' AWS objets IoT, à la liste des ressources avec des balises spécifiques et à la création et à l'utilisation d'un rôle lié à un service pour l'IoT. AWS SiteWise

AWSIoTSiteWiseConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTSiteWiseConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 31 mai 2019, 21:37 UTC
- Heure modifiée : 31 mai 2019, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTSiteWiseFullAccess

Description : fournit un accès complet à l'IoT SiteWise.

AWSIoTSiteWiseFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTSiteWiseFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 décembre 2018, 20:53 UTC
- Heure modifiée : 04 décembre 2018, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTSiteWiseMonitorPortalAccess

Description : Cette politique accorde des autorisations pour accéder aux SiteWise actifs AWS IoT et aux données des actifs, créer des ressources AWS IoT SiteWise Monitor et répertorier les utilisateurs AWS SSO.

AWSIoTSiteWiseMonitorPortalAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTSiteWiseMonitorPortalAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 19 mai 2020, 20:01 UTC
- Heure modifiée : 19 mai 2020, 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTSiteWiseMonitorServiceRolePolicy

Description : Ce rôle confère à AWS IoT SiteWise Monitor les autorisations nécessaires pour accéder à vos SiteWise actifs AWS IoT et à leurs propriétés, et créer des projets AWS IoT SiteWise, des tableaux de bord et des politiques d'accès via des portails AWS IoT SiteWise .

AWSIoTSiteWiseMonitorServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 14 novembre 2019, 00:59 UTC
- Heure modifiée : 13 décembre 2019, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTSiteWiseReadOnlyAccess

Description : fournit un accès en lecture seule à l'IoT SiteWise.

AWSIoTSiteWiseReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTSiteWiseReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 décembre 2018, 20:55 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTThingsRegistration

Description : Cette politique permet aux utilisateurs d'enregistrer des objets en masse à l'aide de l' `StartThingRegistrationTask` API AWS IoT

AWSIoTThingsRegistration est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTThingsRegistration à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 01 décembre 2017, 20:21 UTC

- Heure modifiée : 05 octobre 2020, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "*"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTtwinMakerServiceRolePolicy

Description : permet TwinMaker à AWS IoT d'appeler d'autres AWS services et de synchroniser leurs ressources en votre nom.

AWSIoTtwinMakerServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 13 novembre 2023, 18:59 UTC

- Heure modifiée : 13 novembre 2023, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTtwinMakerServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            ]
        }
    }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTWirelessDataAccess

Description : autorise l'accès aux données d'identité associées aux appareils sans fil AWS IoT.

AWSIoTWirelessDataAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTWirelessDataAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 décembre 2020, 15:31 UTC
- Heure modifiée : 15 décembre 2020, 15:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTWirelessFullAccess

Description : Permet à l'identité associée d'accéder pleinement à toutes les opérations AWS IoT Wireless.

AWSIoTWirelessFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTWirelessFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 décembre 2020, 15:27 UTC
- Heure modifiée : 15 décembre 2020, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTWirelessFullPublishAccess

Description : fournit un accès complet à IoT Wireless pour publier sur IoT Rules Engine en votre nom.

AWSIoTWirelessFullPublishAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTWirelessFullPublishAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 décembre 2020, 15:29 UTC
- Heure modifiée : 15 décembre 2020, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTWirelessGatewayCertManager

Description : autorise l'accès à l'identité associé pour créer, répertorier et décrire des certificats IoT

AWSIoTWirelessGatewayCertManager est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTWirelessGatewayCertManager à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 décembre 2020, 15:30 UTC
- Heure modifiée : 15 décembre 2020, 15:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IoTWirelessGatewayCertManager",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:DescribeCertificate",
        "iot:ListCertificates"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTWirelessLogging

Description : permet à l'identité associée de créer des groupes Amazon CloudWatch Logs et de diffuser des journaux vers ces groupes.

AWSIoTWirelessLogging est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTWirelessLogging à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 décembre 2020, 15:32 UTC
- Heure modifiée : 15 décembre 2020, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessLogging`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIoTWirelessReadOnlyAccess

Description : autorise l'accès en lecture seule de l'identité associée à l' AWS Internet des objets sans fil.

AWSIoTWirelessReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSIoTWirelessReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 décembre 2020, 15:28 UTC
- Heure modifiée : 15 décembre 2020, 15:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIPAMServiceRolePolicy

Description : Permet au gestionnaire d'adresses IP du VPC d'accéder aux ressources du VPC et de s'intégrer aux AWS organisations en votre nom.

AWSIPAMServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 30 novembre 2021, 19:08 UTC
- Heure modifiée : 09 septembre 2026, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
      "*"
    ]
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIQContractServiceRolePolicy

Description : Utilisé par AWS IQ pour exécuter des demandes de paiement pour le compte d'un client

AWSIQContractServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 22 août 2019, 19:28 UTC
- Heure modifiée : 22 août 2019, 19:28 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIQFullAccess

Description : Fournit un accès complet à AWS IQ

AWSIQFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSIQFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 avril 2019, 23:13 UTC
- Heure modifiée : 25 septembre 2019, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIQFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"  
      ]  
    }  
  }  
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSIQPermissionServiceRolePolicy

Description : Permet à AWS IQ de gérer le rôle assumé par les experts AWS IQ.

AWSIQPermissionServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 22 août 2019, 19:36 UTC
- Heure modifiée : 22 août 2019, 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQPermissionServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

Description : Permet d'accéder aux AWS services et aux ressources requis pour les magasins de clés personnalisés AWS KMS

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 14 novembre 2018, 20:10 UTC
- Heure modifiée : 10 novembre 2023, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

Description : permet à AWS KMS de synchroniser les propriétés partagées des clés multirégions.

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 16 juin 2021, 15:37 UTC

- Heure modifiée : 13 novembre 2024, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSKeyManagementServicePowerUser

Description : Permet d'accéder au service de gestion des AWS clés (KMS).

AWSKeyManagementServicePowerUser est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSKeyManagementServicePowerUser` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 07 mars 2017, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSKeyManagementServicePowerUser`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"    
  }  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLakeFormationCrossAccountManager

Description : Fournit un accès multicompte aux ressources de Glue via Lake Formation. Permet également un accès en lecture à d'autres services requis tels que les organisations et le gestionnaire d'accès aux ressources

AWSLakeFormationCrossAccountManagerest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSLakeFormationCrossAccountManager à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 août 2020, 20:59 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLakeFormationDataAdmin

Description : accorde un accès administratif à AWS Lake Formation et à des services connexes, tels que AWS Glue, pour gérer les lacs de données

AWSLakeFormationDataAdmin est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSLakeFormationDataAdmin à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 août 2019, 17:33 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWS Lambda_FullAccess

Description : accorde un accès complet au service AWS Lambda, aux fonctionnalités de la console AWS Lambda et à d'autres services connexes AWS .

AWSLambda_FullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSLambda_FullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 novembre 2020, 21:14 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambda_FullAccess

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWS Lambda_ReadOnlyAccess

Description : accorde un accès en lecture seule au service AWS Lambda, aux fonctionnalités de la console AWS Lambda et à d'autres services associés. AWS

AWSLambda_ReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSLambda_ReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 novembre 2020, 21:10 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLambdaBasicDurableExecutionRolePolicy

Description : fournit des autorisations d'écriture sur les CloudWatch journaux et read/write des autorisations sur les API d'exécution durables utilisées par les fonctions durables Lambda

AWSLambdaBasicDurableExecutionRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSLambdaBasicDurableExecutionRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 02 décembre 2025, 15:04 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaBasicDurableExecutionRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "lambda:CheckpointDurableExecution",
        "lambda:GetDurableExecutionState"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLambdaBasicExecutionRole

Description : fournit des autorisations d'écriture aux CloudWatch journaux.

AWSLambdaBasicExecutionRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSLambdaBasicExecutionRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service

- Heure de création : 09 avril 2015, 15:03 UTC
- Heure modifiée : 09 avril 2015, 15:03 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLambdaDynamoDBExecutionRole

Description : fournit un accès listé et en lecture aux flux DynamoDB et des autorisations d'écriture sur les CloudWatch journaux.

AWSLambdaDynamoDBExecutionRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSLambdaDynamoDBExecutionRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 09 avril 2015, 15:09 UTC
- Heure modifiée : 09 avril 2015, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
```

```
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLambdaENIManagementAccess

Description : fournit les autorisations minimales permettant à une fonction Lambda de gérer les ENI (créer, décrire, supprimer) utilisés par une fonction VPC-enabled Lambda.

AWSLambdaENIManagementAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSLambdaENIManagementAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 06 décembre 2016, 00:37 UTC
- Heure modifiée : 01 octobre 2020, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLambdaExecute

Important

La politique AWSLambdaExecute gérée est sur le point de devenir obsolète et son utilisation avec AWS Lambda n'est plus recommandée. Utilisez à la place [AWSLambdaBasicExecutionRole](#). Lorsque le service IAM finira par déprécier la politique,

vous ne pourrez plus l'associer à un rôle. Cependant, vous pouvez associer un rôle existant à une ressource même si ce rôle utilise la politique obsolète.

Description : fournit un accès Put, Get à S3 et un accès complet aux CloudWatch journaux.

AWSLambdaExecute est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSLambdaExecute à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 06 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaExecute`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:::*"  
    }  
  ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLambdaFullAccess

Description : Cette politique est sur la voie de la dépréciation. Consultez la documentation pour obtenir des conseils : <https://docs.aws.amazon.com/lambda/latest/dg/access-control-identity-based.html>. fournit un accès complet à Lambda, S3, DynamoDB, CloudWatch Metrics et Logs.

AWSLambdaFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSLambdaFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 27 novembre 2017, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaFullAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLambdaInvocation-DynamoDB

Description : fournit un accès en lecture à DynamoDB Streams.

AWSLambdaInvocation-DynamoDB est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSLambdaInvocation-DynamoDB à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 06 février 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
```

```
        "dynamodb:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLambdaInvokeWebFunctionEndpointAccess

Description : accorde l'autorisation d'invoquer les points de terminaison des fonctions Web AWS Lambda.

AWSLambdaInvokeWebFunctionEndpointAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSLambdaInvokeWebFunctionEndpointAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 octobre 2026, 16:47 UTC
- Heure modifiée : 01 octobre 2026, 16:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaInvokeWebFunctionEndpointAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeWebFunctionEndpoint"
      ],
      "Resource" : "arn:aws:lambda:*:*:web-function/*/endpoint/*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLambdaKinesisExecutionRole

Description : fournit un accès listé et en lecture aux flux Kinesis et des autorisations d'écriture pour les CloudWatch journaux.

AWSLambdaKinesisExecutionRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSLambdaKinesisExecutionRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 09 avril 2015, 15:14 UTC
- Heure modifiée : 19 novembre 2018, 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLambdaManagedEC2ResourceOperator

Description : Cette politique accorde des autorisations permettant de créer et d'administrer des ressources EC2 gérées par les instances gérées Lambda, ainsi que des autorisations descriptives.

AWSLambdaManagedEC2ResourceOperator est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSLambdaManagedEC2ResourceOperator à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 novembre 2025, 08:34 UTC
- Heure modifiée : 10 juin 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaManagedEC2ResourceOperator`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLambdaMSKExecutionRole

Description : fournit les autorisations nécessaires pour accéder à MSK Cluster au sein d'un VPC, gérer les ENI (créer, décrire, supprimer) dans le VPC et écrire les autorisations dans les journaux. CloudWatch

AWSLambdaMSKExecutionRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSLambdaMSKExecutionRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 11 août 2020, 17:35 UTC
- Heure modifiée : 02 août 2022, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaMSKExecutionRole`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLambdaNetworkConnectorOperatorPolicy

Description : Cette politique accorde des autorisations pour créer et administrer des ressources ENI gérées par le Lambda Network Connector.

AWSLambdaNetworkConnectorOperatorPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSLambdaNetworkConnectorOperatorPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 juin 2026, 15:27 UTC
- Heure modifiée : 22 juin 2026, 15:27 UTC

- ARN: `arn:aws:iam::aws:policy/AWSLambdaNetworkConnectorOperatorPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  }
}
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLambdaReplicator

Description : accorde à Lambda Replicator les autorisations nécessaires pour répliquer les fonctions entre les régions

AWSLambdaReplicator est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 23 mai 2017, 17:53 UTC
- Heure modifiée : 08 décembre 2017, 00:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
      "*"
    ]
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLambdaRole

Description : stratégie par défaut pour le rôle de service AWS Lambda.

AWSLambdaRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSLambdaRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 06 février 2015, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaRole

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLambdaServiceRolePolicy

Description : permet à Lambda de décrire et de mettre fin aux instances gérées depuis EC2 en votre nom.

AWSLambdaServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle

- Heure de création : 30 novembre 2025, 08:04 UTC
- Heure modifiée : 22 juin 2026, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLambdaSQSQueueExecutionRole

Description : Permet de recevoir des messages, de supprimer des messages et d'accéder aux attributs de lecture aux files d'attente SQS, ainsi que des autorisations d'écriture sur les CloudWatch journaux.

AWSLambdaSQSQueueExecutionRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSLambdaSQSQueueExecutionRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 14 juin 2018, 21:50 UTC
- Heure modifiée : 14 juin 2018, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLambdaVPCAccessExecutionRole

Description : fournit des autorisations minimales pour l'exécution d'une fonction Lambda lors de l'accès à une ressource au sein d'un VPC : création, description, suppression d'interfaces réseau et autorisations d'écriture dans les CloudWatch journaux.

AWSLambdaVPCAccessExecutionRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSLambdaVPCAccessExecutionRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 11 février 2016, 23:15 UTC
- Heure modifiée : 05 janvier 2024, 22:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLicenseManagerConsumptionPolicy

Description : fournit des autorisations pour autoriser l'accès aux actions de l'API AWS License Manager requises pour utiliser les licences auxquelles l'utilisateur a droit.

AWSLicenseManagerConsumptionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSLicenseManagerConsumptionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 11 août 2021, 23:18 UTC

- Heure modifiée : 11 août 2021, 23:18 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
    ],
    "Resource" : "*"
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

Description : permet au service d'abonnements Linux AWS License Manager de gérer les ressources en votre nom.

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 20 décembre 2022, 18:54 UTC
- Heure modifiée : 08 juillet 2024, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLicenseManagerMasterAccountRolePolicy

Description : Politique relative au rôle du compte principal du service AWS License Manager

AWSLicenseManagerMasterAccountRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 26 novembre 2018, 19:03 UTC
- Heure modifiée : 31 mai 2022, 20:50 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            ]
        }
    }
}
}

```

```
]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLicenseManagerMemberAccountRolePolicy

Description : Politique relative au rôle des comptes des membres du service AWS License Manager

AWSLicenseManagerMemberAccountRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 26 novembre 2018, 19:04 UTC
- Heure modifiée : 15 novembre 2019, 22:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
      "*"
    ]
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLicenseManagerServiceRolePolicy

Description : Politique de rôle par défaut du service AWS License Manager

AWSLicenseManagerServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 26 novembre 2018, 19:02 UTC
- Heure modifiée : 19 novembre 2025, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerServiceRolePolicy`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
    "*"
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

Description : Permet au service d'abonnements utilisateur AWS License Manager de gérer les ressources en votre nom.

AWSLicenseManagerUserSubscriptionsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 30 juillet 2022, 01:17 UTC
- Heure modifiée : 10 juillet 2026, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "bz0vcy31ooqlzk5tsash4r1lik",
        "d44g89hc0gp9jdzm99rznthpw",
        "77yzkpa7kveely1tt7wnsdwoc",
        "a8jthu9h8pjsn4b8ylvfl6sfr",
        "7at6der8hnlov1g347e6tdkde",
        "3t0v0vuhvxjzm6m462f9v8iz4",
        "4gs2prcp03ojilgkx8m3ifh7",
        "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-*"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSM2ServicePolicy

Description : Permet à AWS M2 de gérer les AWS ressources en votre nom.

AWSM2ServicePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 07 juin 2022, 20:26 UTC
- Heure modifiée : 07 juin 2022, 20:26 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      ]
    }
  }
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSManagedAccountManagementAccess

Description : accorde des AWS autorisations pour mettre à jour et gérer les rôles AWS gérés pour les comptes AWS gérés

AWSManagedAccountManagementAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSManagedAccountManagementAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 20 juillet 2026, 19:57 UTC
- Heure modifiée : 01 octobre 2026, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedAccountManagementAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSManagedAccountUserEntitlementAccess

Description : accorde des AWS autorisations pour gérer les droits d'accès aux comptes gérés AWS

AWSManagedAccountUserEntitlementAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSManagedAccountUserEntitlementAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 juillet 2026, 21:42 UTC
- Heure modifiée : 17 juillet 2026, 21:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedAccountUserEntitlementAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSManagedAdvancedFeaturesActivationAccess

Description : AWS autorise l'activation des fonctionnalités avancées pour les comptes AWS gérés

AWSManagedAdvancedFeaturesActivationAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSTrustedFeaturesActivationAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 21 juillet 2026, 14:27 UTC
- Heure modifiée : 21 juillet 2026, 14:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedFeaturesActivationAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSManagedBudgetsSpendLimitManagementAccess

Description : accorde au service AWS Budgets l'autorisation de joindre et de détacher des politiques de contrôle des services et de gérer les comptes dans une AWS organisation afin de faire respecter les limites de dépenses sur les comptes des membres.

AWSManagedBudgetsSpendLimitManagementAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSManagedBudgetsSpendLimitManagementAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 juillet 2026, 21:12 UTC
- Heure modifiée : 07 août 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedBudgetsSpendLimitManagementAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSManagedControlPolicyManagementAccess

Description : accorde AWS l'autorisation de gérer les politiques de contrôle de l'organisation pour les comptes AWS gérés

AWSManagedControlPolicyManagementAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSManagedControlPolicyManagementAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 21 juillet 2026, 14:27 UTC
- Heure modifiée : 21 juillet 2026, 14:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedControlPolicyManagementAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSManagedServiceAccessManagementAccess

Description : accorde des autorisations pour gérer les politiques de contrôle des services (SCP) dans les AWS organisations pour le service de gestion de l'accès aux services AWS gérés. Inclut des autorisations pour répertorier, créer, mettre à jour et joindre des SCP relevant des politiques étiquetées avec ManagedBy =service-access.

AWSManagedServiceAccessManagementAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSManagedServiceAccessManagementAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 21 juillet 2026, 17:57 UTC
- Heure modifiée : 21 juillet 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSManagedServiceAccessManagementAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowListRoots",
      "Effect" : "Allow",
      "Action" : "organizations:ListRoots",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSCPLList",
      "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/*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSManagedServices_ContactsServiceRolePolicy

Description : permet aux services AWS gérés de lire les valeurs des balises sur les AWS ressources

AWSManagedServices_ContactsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 23 mars 2023, 17:07 UTC
- Heure modifiée : 23 mars 2023, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_ContactsServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

Description : Services AWS gérés : politique de gestion de l'infrastructure des contrôles de détection

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 19 décembre 2022, 23:11 UTC

- Heure modifiée : 19 décembre 2022, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSManagedServices_EventsServiceRolePolicy

Description : Politique de services AWS gérés pour activer la fonction de traitement d'événements AMS.

AWSManagedServices_EventsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 07 février 2023, 18:41 UTC
- Heure modifiée : 07 février 2023, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSManagedServices_SelfServiceReporting_ServiceRolePolicy

Description : permet à la fonction de création de rapports en libre-service d'Amazon AWS Managed Service de lire les données de AWS l'organisation en votre nom afin de permettre la création de rapports agrégés au niveau de l'organisation

AWSManagedServices_SelfServiceReporting_ServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 08 janvier 2025, 21:22 UTC
- Heure modifiée : 08 janvier 2025, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_SelfServiceReporting_ServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSManagedServicesDeploymentToolkitPolicy

Description : permet aux services AWS gérés de gérer la boîte à outils de déploiement en votre nom.

AWSManagedServicesDeploymentToolkitPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 09 juin 2022, 18:33 UTC
- Heure modifiée : 04 avril 2024, 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSManagedSettingsAdminAccess

Description : accorde un accès administratif complet à la gestion des Compte AWS paramètres. Cette politique permet aux propriétaires de consulter et de modifier les informations de compte, la facturation, les paiements, l'enregistrement fiscal, la gestion de l'identité, les politiques de l'organisation, les budgets, l'analyse des coûts et les notifications relatives à l'espace de travail. Destiné aux propriétaires d'espaces de travail qui ont besoin d'un accès administratif complet pour la configuration du compte et la gestion des membres. La politique n'autorise pas l'accès au calcul, au stockage, à la mise en réseau ou à d'autres services d'infrastructure non liés aux paramètres du compte.

AWSManagedSettingsAdminAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSManagedSettingsAdminAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 juillet 2026, 01:27 UTC
- Heure modifiée : 30 septembre 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedSettingsAdminAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSManagedSettingsReadOnlyAccess

Description : donne aux membres de l'équipe un accès en lecture seule aux AWS paramètres, y compris aux informations sur l'espace de travail et le propriétaire, la composition de l'équipe, le plan et le résumé des dépenses. Il n'autorise pas à modifier la configuration de l'espace de travail ou à gérer la facturation et les paiements.

AWSManagedSettingsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSManagedSettingsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 juillet 2026, 01:12 UTC
- Heure modifiée : 21 août 2026, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedSettingsReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"   
    }  
  ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSManagedSignUpAdminAccess

Description : donne AWS l'autorisation de terminer l'inscription aux comptes AWS gérés.

AWSManagedSignUpAdminAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSManagedSignUpAdminAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 20 juillet 2026, 19:27 UTC
- Heure modifiée : 20 juillet 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSManagedSignUpAdminAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSManagementConsoleAdministratorAccess

Description : fournit un accès complet pour configurer et personnaliser Console de gestion AWS

AWSManagementConsoleAdministratorAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSManagementConsoleAdministratorAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux fonctions
- Heure de création : 14 août 2025, 21:19 UTC
- Heure modifiée : 23 mars 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AWSManagementConsoleAdministratorAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSManagementConsoleBasicUserAccess

Description : donne accès aux Console de gestion AWS fonctionnalités essentielles et aux fonctionnalités d'expérience utilisateur (UX) aux utilisateurs non administratifs.

AWSManagementConsoleBasicUserAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSManagementConsoleBasicUserAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 août 2025, 20:34 UTC
- Heure modifiée : 17 mars 2026, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagementConsoleBasicUserAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMarketplaceAmiIngestion

Description : Permet AWS Marketplace de copier vos Amazon Machine Images (AMI) afin de les répertorier sur AWS Marketplace

AWSMarketplaceAmiIngestion est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMarketplaceAmiIngestion à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 septembre 2020, 20:55 UTC
- Heure modifiée : 25 septembre 2020, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMarketplaceDeploymentServiceRolePolicy

Description : Permet AWS Marketplace de créer et de gérer les paramètres de déploiement des vendeurs pour les produits auxquels vous êtes abonné AWS Marketplace.

AWSMarketplaceDeploymentServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 15 novembre 2023, 23:34 UTC
- Heure modifiée : 15 novembre 2023, 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  }
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMarketplaceDiscoveryFullAccess

Description : fournit un accès complet à l'API AWS Marketplace Discovery pour rechercher et récupérer des informations sur les produits et les prix.

AWSMarketplaceDiscoveryFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMarketplaceDiscoveryFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 mai 2026, 17:12 UTC
- Heure modifiée : 07 mai 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceDiscoveryFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMarketplaceFullAccess

Description : permet de s'abonner et de se désabonner des AWS Marketplace logiciels, permet aux utilisateurs de gérer les instances logicielles de Marketplace à partir de la page « Votre logiciel » de Marketplace et fournit un accès administratif à EC2.

AWSMarketplaceFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMarketplaceFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 février 2015, 17:21 UTC

- Heure modifiée : 11 septembre 2026, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceFullAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            ]
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMarketplaceGetEntitlements

Description : Fournit un accès en lecture à AWS Marketplace Entitlements

AWSMarketplaceGetEntitlements est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSMarketplaceGetEntitlements` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 mars 2017, 19:37 UTC
- Heure modifiée : 05 avril 2024, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSMarketplaceGetEntitlements",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetEntitlements"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMarketplaceImageBuildFullAccess

Description : fournit un accès complet à la fonctionnalité de création d'images AWS Marketplace privées. En plus de créer des images privées, il fournit également des autorisations pour ajouter des balises aux images, lancer et terminer des instances ec2.

AWSMarketplaceImageBuildFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMarketplaceImageBuildFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 31 juillet 2018, 23:29 UTC
- Heure modifiée : 04 mars 2022, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMarketplaceLicenseManagementServiceRolePolicy

Description : Permet d'accéder Services AWS aux ressources utilisées ou gérées par celles-ci AWS Marketplace pour la gestion des licences.

AWSMarketplaceLicenseManagementServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 03 décembre 2020, 08:33 UTC
- Heure modifiée : 03 décembre 2020, 08:33 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMarketplaceManageSubscriptions

Description : Permet de s'abonner et de se désabonner AWS Marketplace du logiciel

AWSMarketplaceManageSubscription est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMarketplaceManageSubscriptions à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 07 mai 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMarketplaceMeteringFullAccess

Description : Fournit un accès complet à AWS Marketplace Metering.

AWSMarketplaceMeteringFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMarketplaceMeteringFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 mars 2016, 22:39 UTC
- Heure modifiée : 17 mars 2016, 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMarketplaceMeteringRegisterUsage

Description : Fournit les autorisations nécessaires pour enregistrer une ressource et suivre son utilisation via le service AWS Marketplace de mesure.

AWSMarketplaceMeteringRegisterUsage est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMarketplaceMeteringRegisterUsage à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 21 novembre 2019, 01:17 UTC
- Heure modifiée : 21 novembre 2019, 01:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMarketplaceProcurementSystemAdminFullAccess

Description : fournit un accès complet à toutes les actions administratives pour une intégration d'AWS Marketplace achats électroniques.

AWSMarketplaceProcurementSystemAdminFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMarketplaceProcurementSystemAdminFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 juin 2019, 13:07 UTC

- Heure modifiée : 21 avril 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceProcurementSystemAdminFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMarketplacePurchaseOrdersServiceRolePolicy

Description : Permet d'accéder aux AWS Marketplace services de gestion des bons de commande.

AWSMarketplacePurchaseOrdersServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 27 octobre 2021, 15:12 UTC
- Heure modifiée : 27 octobre 2021, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplacePurchaseOrdersServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
    "Effect" : "Allow",
    "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
    ],
    "Resource" : [
        "*"
    ]
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMarketplaceRead-only

Description : Permet de consulter les AWS Marketplace abonnements

AWSMarketplaceRead-only est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMarketplaceRead-only à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 07 mai 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceRead-only`

Version de la politique

Version de la politique : v13 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMarketplaceResaleAuthorizationServiceRolePolicy

Description : Permet d'accéder Services AWS aux ressources utilisées ou gérées par celles-ci AWS Marketplace pour l'autorisation de revente.

AWSMarketplaceResaleAuthorizationServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 05 mars 2024, 18:47 UTC
- Heure modifiée : 01 août 2025, 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceResaleAuthorizationServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"  
    }  
  ]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMarketplaceSellerFullAccess

Description : fournit un accès complet à toutes les opérations des vendeurs sur le site AWS Marketplace et à d'autres AWS services tels que la gestion des AMI.

AWSMarketplaceSellerFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMarketplaceSellerFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 juillet 2019, 20:40 UTC
- Heure modifiée : 12 août 2026, 16:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess`

Version de la politique

Version de la politique : v33 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"    
  }  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMarketplaceSellerOfferManagement

Description : permet aux vendeurs d'accéder aux activités de gestion des offres et des contrats.

AWSMarketplaceSellerOfferManagement est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMarketplaceSellerOfferManagement à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 novembre 2024, 00:41 UTC
- Heure modifiée : 31 mars 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerOfferManagement`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMarketplaceSellerProductsFullAccess

Description : fournit aux vendeurs un accès complet à AWS Marketplace la page Produits de gestion et à d'autres AWS services tels que la gestion des AMI.

AWSMarketplaceSellerProductsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMarketplaceSellerProductsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 juillet 2019, 21:06 UTC
- Heure modifiée : 19 février 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess`

Version de la politique

Version de la politique : v15 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMarketplaceSellerProductsReadOnly

Description : Fournissez aux vendeurs un accès en lecture seule à la page Produits AWS Marketplace de gestion.

AWSMarketplaceSellerProductsReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSMarketplaceSellerProductsReadOnly` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 juillet 2019, 21:40 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMcpServiceActionsFullAccess

Description : fournit un accès complet à toutes les actions de service MCP. Cette politique n'autorise pas l'accès aux actions entreprises par le MCP, mais uniquement aux actions du MCP elles-mêmes.

AWSMcpServiceActionsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMcpServiceActionsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 21 novembre 2025, 22:49 UTC

- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: arn:aws:iam::aws:policy/AWSMcpServiceActionsFullAccess

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllMCPServiceActions",
      "Effect" : "Allow",
      "Action" : "*",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:IsMcpServiceAction" : "true"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMCPSignInOAuthAccessPolicy

Description : Fournit un accès pour s'authentifier auprès du serveur AWS MCP à l'aide d'OAuth AWS Sign-In

AWSMCPSignInOAuthAccessPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMCPSignInOAuthAccessPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 juillet 2026, 06:57 UTC
- Heure modifiée : 09 juillet 2026, 06:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMCPSignInOAuthAccessPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMediaConnectServicePolicy

Description : politique par défaut qui autorise l'accès Services AWS aux ressources utilisées ou gérées par MediaConnect.

AWSMediaConnectServicePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 03 avril 2023, 22:11 UTC
- Heure modifiée : 29 octobre 2025, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMediaLiveAnywhereServiceRolePolicy

Description : permet à MediaLive Anywhere de créer et de gérer AWS des ressources en votre nom.

AWSMediaLiveAnywhereServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 14 avril 2025, 22:07 UTC
- Heure modifiée : 14 avril 2025, 22:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaLiveAnywhereServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
  ]
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMediaTailorServiceRolePolicy

Description : Permettre l'accès aux AWS ressources utilisées ou gérées par MediaTailor

AWSMediaTailorServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 17 septembre 2021, 22:27 UTC
- Heure modifiée : 17 septembre 2021, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    }
  ]
}
```


En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMigrationHubDiscoveryAccess

Description : La politique AWSMigrationHubService permet d'appeler AWSApplicationDiscoveryService au nom du client.

AWSMigrationHubDiscoveryAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMigrationHubDiscoveryAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 14 août 2017, 13:30 UTC
- Heure modifiée : 06 août 2020, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
      "*"
    ]
  }
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMigrationHubDMSAccess

Description : Politique selon laquelle le service de migration de base de données doit jouer un rôle dans le compte du client pour appeler Migration Hub

AWSMigrationHubDMSAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMigrationHubDMSAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 14 août 2017, 14:00 UTC
- Heure modifiée : 07 octobre 2019, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMigrationHubFullAccess

Description : Politique gérée pour fournir au client l'accès au service Migration Hub

AWSMigrationHubFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMigrationHubFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 août 2017, 14:02 UTC
- Heure modifiée : 19 juin 2019, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ]
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMigrationHubOrchestratorConsoleFullAccess

Description : fournit un accès limité à AWS Migration Hub, AWS Application Discovery Service, Amazon Simple Storage Service et AWS Secrets Manager. Cette politique accorde également un accès complet au service AWS Migration Hub Orchestrator.

AWSMigrationHubOrchestratorConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMigrationHubOrchestratorConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 avril 2022, 02:26 UTC
- Heure modifiée : 05 décembre 2023, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MH0",
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-orchestrator:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListAllMyBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "S3MH0",
      "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*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMigrationHubOrchestratorInstanceRolePolicy

Description : Cette politique doit être jointe pour les instances migrées SAP et MGN afin que notre service puisse orchestrer les instances en téléchargeant des scripts depuis S3 et pour récupérer des valeurs secrètes dans l'instance EC2.

AWSMigrationHubOrchestratorInstanceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMigrationHubOrchestratorInstanceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 avril 2022, 02:43 UTC
- Heure modifiée : 20 avril 2022, 02:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorInstanceRolePolicy

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*/*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMigrationHubOrchestratorPlugin

Description : fournit un accès limité à Amazon Simple Storage Service, à AWS Secrets Manager et aux actions liées au plug-in pour AWS Migration Hub Orchestrator.

AWSMigrationHubOrchestratorPluginest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMigrationHubOrchestratorPlugin à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 avril 2022, 02:25 UTC
- Heure modifiée : 20 avril 2022, 02:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMigrationHubOrchestratorServiceRolePolicy

Description : fournit les autorisations nécessaires à Migration Hub Orchestrator pour migrer et moderniser vos charges de travail sur site

AWSMigrationHubOrchestratorServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 20 avril 2022, 02:24 UTC
- Heure modifiée : 04 mars 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubOrchestratorServiceRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
    }
  }
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMigrationHubRefactorSpaces- EnvironmentsWithoutBridgesFullAccess

Description : accorde un accès complet aux espaces de refactorisation de AWS Migration Hub et à d'autres services AWS connexes, à l'exception de AWS Transit Gateway et des groupes de sécurité EC2 qui ne sont pas requis lors de l'utilisation d'environnements sans pont réseau. Cette politique exclut également les autorisations requises pour AWS Lambda et AWS Resource Access Manager, car elles peuvent être réduites en fonction des balises.

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 avril 2023, 20:09 UTC
- Heure modifiée : 11 avril 2024, 18:16 UTC

- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

Description : à utiliser dans le rôle de service IAM transmis au document SSM Automation AWSRefactorSpaces-CreateResources pour accorder les autorisations nécessaires à l'exécution de l'automatisation. La politique autorise l' read/write accès aux balises EC2 afin de suivre les progrès de l'automatisation. Lorsque le pont réseau de l'environnement Refactor Spaces est activé, l'automatisation ajoute également le groupe de sécurité de l'environnement à l'instance EC2 pour autoriser le trafic provenant d'autres services Refactor Spaces de l'environnement. La politique donne également accès aux paramètres SSM des actions post-lancement du service de migration des applications.

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMigrationHubRefactorSpaces-SSMAutomationPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 10 août 2023, 15:08 UTC
- Heure modifiée : 10 août 2023, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-
*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMigrationHubRefactorSpacesFullAccess

Description : accorde un accès complet à AWS MigrationHub Refactor Spaces, aux fonctionnalités de la console AWS MigrationHub Refactor Spaces et à d'autres AWS services connexes, à l'exception des autorisations requises pour AWS Lambda et AWS Resource Access Manager, car leur portée peut être réduite en fonction des balises.

AWSMigrationHubRefactorSpacesFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMigrationHubRefactorSpacesFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2021, 07:12 UTC
- Heure modifiée : 11 avril 2024, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMigrationHubRefactorSpacesServiceRolePolicy

Description : donne accès aux AWS ressources gérées ou utilisées par AWS Migration Hub Refactor Spaces.

AWSMigrationHubRefactorSpacesServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 29 novembre 2021, 06:50 UTC
- Heure modifiée : 20 juillet 2023, 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMigrationHubSMSAccess

Description : Politique selon laquelle le service de migration de serveurs doit jouer un rôle dans le compte du client pour appeler Migration Hub

AWSMigrationHubSMSAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMigrationHubSMSAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 14 août 2017, 13:57 UTC
- Heure modifiée : 07 octobre 2019, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMigrationHubStrategyCollector

Description : accorde des autorisations pour autoriser la communication avec le service AWS Migration Hub Strategy Recommendations, l'accès read/write aux compartiments S3 liés au service, l'accès à Amazon API Gateway pour télécharger les journaux et les métriques AWS, l'accès à AWS Secrets Manager pour récupérer les informations d'identification et tous les services associés.

AWSMigrationHubStrategyCollector est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMigrationHubStrategyCollector à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 octobre 2021, 20:15 UTC
- Heure modifiée : 01 avril 2024, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMigrationHubStrategyConsoleFullAccess

Description : Donne un accès complet au service de recommandations stratégiques du AWS Migration Hub et l'accès aux AWS services connexes via le Console de gestion AWS.

AWSMigrationHubStrategyConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMigrationHubStrategyConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 octobre 2021, 20:13 UTC
- Heure modifiée : 09 novembre 2022, 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMigrationHubStrategyServiceRolePolicy

Description : Activez l'accès aux AWS ressources utilisées ou gérées par le service AWS Migration Hub Strategy Recommendations.

AWSMigrationHubStrategyServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 19 octobre 2021, 20:02 UTC
- Heure modifiée : 19 octobre 2021, 20:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubStrategyServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMobileHub_FullAccess

Description : Cette politique peut être associée à n'importe quel utilisateur, rôle ou groupe, afin d'autoriser les utilisateurs à créer, supprimer et modifier des projets (et leurs AWS ressources associées) dans AWS Mobile Hub. Cela inclut également les autorisations nécessaires pour générer et télécharger des exemples de code source d'application mobile pour chaque projet Mobile Hub.

AWSMobileHub_FullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMobileHub_FullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 janvier 2016, 19:56 UTC
- Heure modifiée : 19 décembre 2019, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_FullAccess`

Version de la politique

Version de la politique : v14 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMobileHub_ReadOnly

Description : Cette politique peut être associée à n'importe quel utilisateur, rôle ou groupe, afin d'autoriser les utilisateurs à répertorier et à consulter des projets dans AWS Mobile Hub. Cela inclut également les autorisations nécessaires pour générer et télécharger des exemples de code source d'application mobile pour chaque projet Mobile Hub. Il ne permet pas à l'utilisateur de modifier la configuration d'un projet Mobile Hub.

AWSMobileHub_ReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMobileHub_ReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 janvier 2016, 19:55 UTC
- Heure modifiée : 23 juillet 2018, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_ReadOnly`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSMSKReplicatorExecutionRole

Description : accorde des autorisations à Amazon MSK Replicator pour répliquer les données entre les clusters MSK.

AWSMSKReplicatorExecutionRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSMSKReplicatorExecutionRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 06 décembre 2023, 00:07 UTC
- Heure modifiée : 25 mars 2024, 21:36 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*/*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSNATGatewayServiceRolePolicy

Description : fournit des autorisations pour gérer les ressources VPC pour la configuration et la gestion des passerelles NAT.

AWSNATGatewayServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 14 novembre 2025, 17:19 UTC
- Heure modifiée : 14 novembre 2025, 17:19 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNATGatewayServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSNetworkFirewallFullAccess

Description : accorde un accès complet au service AWS Network Firewall, y compris des autorisations pour créer, configurer, gérer et supprimer des ressources, des politiques et des groupes

de règles de pare-feu. Inclut également des autorisations pour modifier les points de terminaison VPC, les politiques de compartiment S3, les configurations CloudWatch des journaux et la création de rôles liés aux services pour le pare-feu réseau et les services de diffusion de journaux

AWSNetworkFirewallFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSNetworkFirewallFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 10 juin 2025, 21:52 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkFirewallFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSNetworkFirewallReadOnlyAccess

Description : fournit un accès en lecture seule aux ressources AWS du pare-feu réseau via l'interface de ligne de Console de gestion AWS commande et les kits SDK. Cette politique permet aux utilisateurs de visualiser et de surveiller les configurations de pare-feu, les politiques, les groupes de règles et les ressources associées, sans qu'il soit possible d'apporter des modifications.

AWSNetworkFirewallReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSNetworkFirewallReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 10 juin 2025, 21:52 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkFirewallReadOnlyAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*:*:*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSNetworkFirewallServiceRolePolicy

Description : Permet AWSNetworkFirewall de créer et de gérer les ressources nécessaires à vos pare-feux.

AWSNetworkFirewallServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 17 novembre 2020, 17:17 UTC
- Heure modifiée : 01 juin 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkFirewallServiceRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*/*"
]
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSNetworkManagerCloudWANServiceRolePolicy

Description : NetworkManager Autoriser l'accès aux ressources associées à votre réseau central

AWSNetworkManagerCloudWANServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 12 juillet 2022, 12:17 UTC
- Heure modifiée : 12 juillet 2022, 12:17 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:DeleteTransitGatewayRouteTableAnnouncement",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:DisableTransitGatewayRouteTablePropagation"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSNetworkManagerFullAccess

Description : fournit un accès complet à Amazon NetworkManager via le Console de gestion AWS.

AWSNetworkManagerFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSNetworkManagerFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 décembre 2019, 17:37 UTC
- Heure modifiée : 03 décembre 2019, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "networkmanager:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "networkmanager.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSNetworkManagerReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon NetworkManager via le Console de gestion AWS.

AWSNetworkManagerReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSNetworkManagerReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 décembre 2019, 17:35 UTC
- Heure modifiée : 03 décembre 2019, 17:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "networkmanager:Describe*",
      "networkmanager:Get*",
      "networkmanager:List*"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSNetworkManagerServiceRolePolicy

Description : NetworkManager Autoriser l'accès aux ressources associées à vos réseaux mondiaux

AWSNetworkManagerServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 03 décembre 2019, 14:03 UTC
- Heure modifiée : 27 juillet 2022, 19:41 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerServiceRolePolicy

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"br/>  }  
]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSObservabilityAdminLogsCentralizationServiceRolePolicy

Description : autorisations de Service-linked rôle pour la CloudWatch centralisation des journaux

AWSObservabilityAdminLogsCentralizationServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 15 septembre 2025, 14:34 UTC
- Heure modifiée : 15 septembre 2025, 14:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminLogsCentralizationServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSObservabilityAdminServiceRolePolicy

Description : donne accès à la gestion de l'enregistreur de AWS configuration de configuration, à la gestion de l'agrégateur de AWS configuration de configuration, à la création AWS d'un rôle lié au service de configuration pour la fonctionnalité de l'enregistreur de configuration, à la consommation des données de configuration de l'enregistreur et à la lecture AWS des données des organisations pour les fonctionnalités organisationnelles.

AWSObservabilityAdminServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 27 novembre 2024, 19:36 UTC
- Heure modifiée : 14 juillet 2026, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSObservabilityAdminTelemetryEnablementServiceRolePolicy

Description : Permet de gérer les ressources de l'enregistreur AWS Config et les paramètres de télémétrie relatifs aux AWS ressources, y compris les journaux et les métriques.

AWSObservabilityAdminTelemetryEnablementServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 01 août 2025, 18:04 UTC
- Heure modifiée : 23 septembre 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminTelemetryEnablementServiceRolePolicy`

Version de la politique

Version de la politique : v15 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "TelemetryOperationsFor0TelEnrichmentSimba",
    "Effect" : "Allow",
    "Action" : [
      "observabilityadmin:GetTelemetryEnrichmentStatus",
      "observabilityadmin:StartTelemetryEnrichment",
      "observabilityadmin:StopTelemetryEnrichment"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "TelemetryOperationsFor0TelEnrichmentResourceExplorer",
    "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" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "TelemetryOperationsFor0TelEnrichmentCloudWatch",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:Get0TelEnrichment",
      "cloudwatch:Start0TelEnrichment"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "TelemetryOperationsFor0TelEnrichmentSLR",
    "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/
CloudWatchTelemetryRuleEKSAaddonRoleTemplate:1"
    },
    {
      "Sid" : "AcquireRoleFromTemplate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/
CloudWatchTelemetryRuleEKSAaddonRole",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:RoleTemplateARN" : "arn:aws:iam::aws:role-
template/telemetry-enablement.observabilityadmin.amazonaws.com/
CloudWatchTelemetryRuleEKSAaddonRoleTemplate:1"
        }
      }
    },
    {
      "Sid" : "AttachManagedPolicyFromTemplate",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Resource" : "arn:aws:iam::*:role/service-role/
CloudWatchTelemetryRuleEKSAaddonRole",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:RoleTemplateARN" : "arn:aws:iam::aws:role-
template/telemetry-enablement.observabilityadmin.amazonaws.com/
CloudWatchTelemetryRuleEKSAaddonRoleTemplate: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}"
        }
      }
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSOrganizationsFullAccess

Description : fournit un accès complet aux AWS organisations.

AWSOrganizationsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSOrganizationsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 novembre 2018, 20:31 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC

- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsFullAccess`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSOrganizationsReadOnlyAccess

Description : fournit un accès en lecture seule aux organisations. AWS

AWSOrganizationsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSOrganizationsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 novembre 2018, 20:32 UTC
- Heure modifiée : 07 juin 2024, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSOrganizationsServiceTrustPolicy

Description : politique permettant aux AWS organisations de partager leur confiance avec d'autres personnes approuvées dans le Services AWS but de simplifier la configuration des clients.

AWSOrganizationsServiceTrustPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 10 octobre 2017, 23:04 UTC
- Heure modifiée : 05 mars 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOrganizationsServiceTrustPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSOutpostsAuthorizeServerPolicy

Description : Cette politique accorde des autorisations qui vous permettent d'installer un serveur Outpost sur votre réseau local.

AWSOutpostsAuthorizeServerPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSOutpostsAuthorizeServerPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 janvier 2023, 19:23 UTC

- Heure modifiée : 04 janvier 2023, 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSOutpostsServiceRolePolicy

Description : Politique relative aux rôles liés aux services pour permettre l'accès aux AWS ressources gérées par AWS Outposts

AWSOutpostsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 09 novembre 2020, 22:55 UTC
- Heure modifiée : 17 avril 2025, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOutpostsServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ]
  }
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPanoramaApplianceRolePolicy

Description : permet au logiciel AWS IoT d'une appliance AWS Panorama de télécharger des journaux sur Amazon CloudWatch.

AWSPanoramaApplianceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPanoramaApplianceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 01 décembre 2020, 13:13 UTC
- Heure modifiée : 01 décembre 2020, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPanoramaApplianceServiceRolePolicy

Description : permet à une appliance AWS Panorama de télécharger des journaux sur Amazon CloudWatch et d'obtenir des objets à partir de points d'accès Amazon S3 créés pour être utilisés avec AWS Panorama.

AWSPanoramaApplianceServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPanoramaApplianceServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 20 octobre 2021, 12:14 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
        }
    }
}

```

```
}  
  }  
    }  
      ]  
    }  
  }
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPanoramaFullAccess

Description : Fournit un accès complet à AWS Panorama

AWSPanoramaFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPanoramaFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2020, 13:12 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPanoramaFullAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPanoramaGreengrassGroupRolePolicy

Description : autorise une fonction AWS Lambda sur une appliance AWS Panorama à gérer les ressources dans Panorama, à télécharger des journaux et des métriques sur Amazon CloudWatch et à gérer des objets dans des compartiments créés pour être utilisés avec Panorama.

AWSPanoramaGreengrassGroupRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPanoramaGreengrassGroupRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 01 décembre 2020, 13:10 UTC
- Heure modifiée : 06 janvier 2021, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
      "*"
    ]
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPanoramaSageMakerRolePolicy

Description : Permet SageMaker à Amazon de gérer des objets dans des compartiments créés pour être utilisés avec AWS Panorama.

AWSPanoramaSageMakerRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPanoramaSageMakerRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 01 décembre 2020, 13:13 UTC
- Heure modifiée : 01 décembre 2020, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucket*"
      ],
    },
  ],
}
```

```
    "Resource" : [
      "arn:aws:s3:::*aws-panorama*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPanoramaServiceLinkedRolePolicy

Description : Permet à AWS Panorama de gérer les ressources dans AWS IoT, AWS Secrets Manager et AWS Panorama.

AWSPanoramaServiceLinkedRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 20 octobre 2021, 12:12 UTC
- Heure modifiée : 20 octobre 2021, 12:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
    ]
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPanoramaServiceRolePolicy

Description : permet à AWS Panorama de gérer les ressources dans Amazon S3, AWS IoT, AWS IoT GreenGrass, AWS Lambda SageMaker, Amazon et Amazon CloudWatch Logs, et de transmettre des rôles de service à AWS IoT GreenGrass, AWS IoT et Amazon SageMaker.

AWSPanoramaServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSPanoramaServiceRolePolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 01 décembre 2020, 13:14 UTC
- Heure modifiée : 01 décembre 2020, 13:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPartnerCentralChannelHandshakeApprovalManagement

Description : fournit l'accès nécessaire aux activités de gestion des approbations liées à la prise de contact des chaînes.

AWSPartnerCentralChannelHandshakeApprovalManagement est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPartnerCentralChannelHandshakeApprovalManagement à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 19 novembre 2025, 16:34 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralChannelHandshakeApprovalManagement`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ChannelHandshakeManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListChannelHandshakes",
        "partnercentral:AcceptChannelHandshake",
        "partnercentral:RejectChannelHandshake"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    }
  ]
}
```


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPartnerCentralChannelManagement

Description : fournit l'accès nécessaire aux activités de gestion des chaînes.

AWSPartnerCentralChannelManagement est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPartnerCentralChannelManagement à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 novembre 2025, 16:34 UTC
- Heure modifiée : 14 février 2026, 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralChannelManagement`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPartnerCentralFullAccess

Description : fournit un accès complet à AWS Partner Central et aux applications connexes Services AWS.

AWSPartnerCentralFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPartnerCentralFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 novembre 2024, 23:33 UTC
- Heure modifiée : 12 mars 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralFullAccess`

Version de la politique

Version de la politique : v14 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPartnerCentralMarketingManagement

Description : fournit l'accès nécessaire aux activités de marketing.

AWSPartnerCentralMarketingManagement est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPartnerCentralMarketingManagement à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2025, 00:34 UTC
- Heure modifiée : 14 février 2026, 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralMarketingManagement`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPartnerCentralOpportunityManagement

Description : fournit l'accès nécessaire aux activités de gestion des opportunités.

AWSPartnerCentralOpportunityManagement est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPartnerCentralOpportunityManagement à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 novembre 2024, 19:09 UTC
- Heure modifiée : 16 juin 2026, 13:27 UTC

- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralOpportunityManagement`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPartnerCentralRevenueAttributionManagement

Description : fournit l'accès nécessaire aux activités de gestion de l'attribution des recettes.

AWSPartnerCentralRevenueAttributionManagement est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSPartnerCentralRevenueAttributionManagement` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 juin 2026, 19:12 UTC
- Heure modifiée : 30 juin 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralRevenueAttributionManagement`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}

```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPartnerCentralSandboxFullAccess

Description : fournit l'accès nécessaire aux tests pour les développeurs dans le catalogue Sandbox.

AWSPartnerCentralSandboxFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPartnerCentralSandboxFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 novembre 2024, 19:10 UTC
- Heure modifiée : 12 mars 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralSandboxFullAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy

Description : donne accès à la lecture ResourceSnapshotJob d'une ressource et à sa capture d'écran dans l'engagement cible.

AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer

AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 10 décembre 2024, 18:21 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPartnerLedSupportReadOnlyAccess

Description : Cette politique peut être utilisée pour accorder un accès en lecture seule aux API capables de lire les métadonnées des services de votre. Compte AWS Vous pouvez utiliser cette politique pour permettre à vos partenaires du programme de Partner-Led support d'accéder aux services spécifiés dans la section relative aux autorisations ci-dessous.

AWSPartnerLedSupportReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPartnerLedSupportReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 novembre 2024, 20:06 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerLedSupportReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPartnerProServeToolsFullAccess

Description : fournit un accès complet aux ProServe outils.

AWSPartnerProServeToolsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPartnerProServeToolsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 mars 2026, 21:57 UTC
- Heure modifiée : 23 mars 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerProServeToolsFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
          ]
        }
      }
    }
  ]
}
```

```
}  
  }  
    }  
  ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPartnerProServeToolsIndividualContributor

Description : Permet de créer et de gérer ses propres évaluations dans des ProServe outils.

AWSPartnerProServeToolsIndividualContributor est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPartnerProServeToolsIndividualContributor à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 mars 2026, 21:57 UTC
- Heure modifiée : 23 mars 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerProServeToolsIndividualContributor`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowProServeToolsIndividualContributorAccess",
      "Effect" : "Allow",
      "Action" : "partnercentral-account-management:AccessProServeTools",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "partnercentral-account-management:ProServeRole" : [
            "AssessmentIndividualContributor"
          ]
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPartnerProServeToolsOrganizationReaderIndividualContributor

Description : Fournit un accès en lecture aux évaluations organisationnelles avec la possibilité de gérer ses propres évaluations.

AWSPartnerProServeToolsOrganizationReaderIndividualContributor est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer

`AWSPartnerProServeToolsOrganizationReaderIndividualContributor` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 mars 2026, 22:12 UTC
- Heure modifiée : 23 mars 2026, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerProServeToolsOrganizationReaderIndividualContributor`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
          ]
        }
      }
    }
  ]
}
```

```
}  
  }  
  ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPCSComputeNodePolicy

Description : autorise les nœuds de calcul AWS PCS à se connecter aux clusters AWS PCS.

AWSPCSComputeNodePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPCSComputeNodePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 juin 2025, 18:07 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPCSComputeNodePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPCSServiceRolePolicy

Description : accorde à PCS l'autorisation de gérer les ressources en votre nom.

AWSPCSServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 27 août 2024, 16:01 UTC
- Heure modifiée : 30 septembre 2026, 18:07 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPCSServiceRolePolicy`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "PermissionsToTerminatePCSMangedInstances",
    "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}"
    }
  }
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPriceListServiceFullAccess

Description : Fournit un accès complet au service de liste de AWS prix.

AWSPriceListServiceFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPriceListServiceFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 novembre 2017, 00:36 UTC
- Heure modifiée : 02 juillet 2024, 13:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPriateCAAuditor

Description : Permet à l'auditeur d'accéder à AWS une autorité de certification privée

AWSPriateCAAuditor est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPriateCAAuditor à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 février 2023, 18:33 UTC
- Heure modifiée : 14 février 2023, 18:33 UTC

- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAAuditor`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPriateCAConnectorForKubernetesPolicy

Description : accorde les autorisations essentielles au connecteur CA AWS privé pour Kubernetes.

AWSPriateCAConnectorForKubernetesPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPriateCAConnectorForKubernetesPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 mai 2025, 19:22 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPriateCAConnectorForKubernetesPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPRivateCAFullAccess

Description : Fournit un accès complet à l'autorité de certification AWS privée

AWSPRivateCAFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPRivateCAFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 février 2023, 18:20 UTC
- Heure modifiée : 14 février 2023, 18:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPRivateCAFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPrivateCAPrivilegedUser

Description : fournit aux utilisateurs de certificats un accès privilégié à l'autorité de certification AWS privée

AWSPrivateCAPrivilegedUser est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSPriateCAPrivilegedUser` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 février 2023, 18:26 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPriateCAPrivilegedUser`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPrivateCAReadOnly

Description : fournit un accès en lecture seule à l'autorité de certification AWS privée

AWSPRivateCAReADOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPRivateCAReADOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 février 2023, 18:30 UTC
- Heure modifiée : 14 février 2023, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPRivateCAReADOnly`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPrivateCAUser

Description : Fournit aux utilisateurs du certificat un accès à AWS une autorité de certification privée

AWSPrivateCAUser est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPrivateCAUser à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 février 2023, 18:16 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAUser`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPrivateMarketplaceAdminFullAccess

Description : Fournit un accès complet à toutes les actions administratives d'un marché AWS privé.

AWSPrivateMarketplaceAdminFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPrivateMarketplaceAdminFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 novembre 2018, 16:32 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPrivateMarketplaceRequests

Description : Permet de créer des demandes sur un marché AWS privé.

AWSPrivateMarketplaceRequestsest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSPriateMarketplaceRequests` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 octobre 2019, 21:44 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPriateMarketplaceRequests`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPrivateNetworksServiceRolePolicy

Description : Permet au service des réseaux AWS privés de gérer les ressources pour le compte du client.

AWSPrivateNetworksServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 16 décembre 2021, 23:17 UTC
- Heure modifiée : 16 décembre 2021, 23:17 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Private5G"
        }
      }
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSProtonCodeBuildProvisioningBasicAccess

Description : Les autorisations CodeBuild doivent exécuter une version pour AWS Proton CodeBuild Provisioning.

AWSProtonCodeBuildProvisioningBasicAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSProtonCodeBuildProvisioningBasicAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 novembre 2022, 21:04 UTC
- Heure modifiée : 09 novembre 2022, 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*:*:*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSProtonCodeBuildProvisioningServiceRolePolicy

Description : Permet à AWS Proton de gérer l'approvisionnement des ressources Proton en utilisant CodeBuild et d'autres AWS services en votre nom.

AWSProtonCodeBuildProvisioningServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 09 novembre 2022, 21:32 UTC
- Heure modifiée : 17 mai 2023, 16:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSProtonDeveloperAccess

Description : donne accès aux API AWS Proton et à la console de gestion, mais n'autorise pas l'administration de modèles ou d'environnements Proton.

AWSProtonDeveloperAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSProtonDeveloperAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 février 2021, 19:02 UTC

- Heure modifiée : 06 juin 2024, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonDeveloperAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSProtonFullAccess

Description : fournit un accès complet aux API AWS Proton et à la console de gestion. Outre ces autorisations, l'accès à Amazon S3 est également nécessaire pour enregistrer des ensembles de modèles à partir de vos compartiments S3, ainsi que l'accès à Amazon IAM pour créer et gérer les rôles de service pour Proton.

AWSProtonFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSProtonFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 février 2021, 19:07 UTC
- Heure modifiée : 06 juin 2024, 18:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            }
        }
    }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSProtonReadOnlyAccess

Description : fournit un accès en lecture seule aux API AWS Proton et à la console de gestion.

AWSProtonReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSProtonReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 février 2021, 19:09 UTC
- Heure modifiée : 18 novembre 2022, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSProtonServiceGitSyncServiceRolePolicy

Description : Politique qui permet à AWS Proton de synchroniser les définitions de votre service, de votre environnement et de vos composants depuis votre référentiel git avec AWS Proton.

AWSProtonServiceGitSyncServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 04 avril 2023, 15:55 UTC
- Heure modifiée : 04 avril 2023, 15:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSProtonSyncServiceRolePolicy

Description : Politique qui permet à AWS Proton de synchroniser le contenu de votre référentiel git avec Proton ou de synchroniser le contenu Proton avec vos référentiels git.

AWSProtonSyncServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle

- Heure de création : 23 novembre 2021, 21:14 UTC
- Heure modifiée : 05 mai 2024, 01:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSPurchaseOrdersServiceRolePolicy

Description : autorise l'affichage et la modification des bons de commande sur la console de facturation

AWSPurchaseOrdersServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSPurchaseOrdersServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 mai 2020, 18:15 UTC

- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSetupCFGCPacksPermissionsBoundary

Description : La AWSQuickSetupCFGCPacksPermissionsBoundary politique définit la liste des autorisations autorisées dans un rôle IAM créé par Quick Setup. Quick Setup utilise un rôle créé avec cette politique pour déployer les packs de conformité AWS Config.

AWSQuickSetupCFGCPacksPermissionsBoundary est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSetupCFGCPacksPermissionsBoundary à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 juin 2024, 09:52 UTC
- Heure modifiée : 26 juin 2024, 09:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupCFGCPacksPermissionsBoundary`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      ]
    }
  ]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSetupDeploymentRolePolicy

Description : fournit des autorisations permettant à AWS Systems Manager Quick Setup de déployer plusieurs types de configuration. Les types de configuration suivants créent des rôles et des automatisations IAM qui configurent rapidement les services et fonctions Amazon Web Services fréquemment utilisés avec les bonnes pratiques recommandées.

AWSQuickSetupDeploymentRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSetupDeploymentRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 juin 2024, 09:55 UTC
- Heure modifiée : 07 septembre 2026, 15:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupDeploymentRolePolicy`

Version de la politique

Version de la politique : v14 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSetupDevOpsGuruPermissionsBoundary

Description : La AWSQuickSetupDevOpsGuruPermissionsBoundary politique définit la liste des autorisations autorisées dans un rôle IAM créé par Quick Setup. La configuration rapide utilise un rôle créé avec cette politique pour activer et configurer Amazon DevOps Guru. Cette politique fournit également des autorisations pour activer Systems Manager Explorer.

AWSQuickSetupDevOpsGuruPermissionsBoundary est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSQuickSetupDevOpsGuruPermissionsBoundary` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 juin 2024, 09:44 UTC
- Heure modifiée : 26 juin 2024, 09:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupDevOpsGuruPermissionsBoundary`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSetupDistributorPermissionsBoundary

Description : QuickSetup crée des rôles IAM qui lui permettent de configurer la fonctionnalité Systems Manager Distributor en votre nom, et utilise cette politique lors de la création de tels rôles pour définir la limite de leurs autorisations.

AWSQuickSetupDistributorPermissionsBoundary est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSetupDistributorPermissionsBoundary à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 juin 2024, 09:50 UTC
- Heure modifiée : 26 juin 2024, 09:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupDistributorPermissionsBoundary`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSetupEnableAREXExecutionPolicy

Description : Cette politique accorde des autorisations qui permettent à Systems Manager d'exécuter le runbook AWSQuickSetupType-EnableAREX d'automatisation, ce qui permet à AWS Resource Explorer d'être utilisé avec Systems Manager.

AWSQuickSetupEnableAREXExecutionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSetupEnableAREXExecutionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 novembre 2024, 22:45 UTC
- Heure modifiée : 15 novembre 2024, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupEnableAREXExecutionPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSetupEnableDHMCExecutionPolicy

Description : Cette politique accorde des autorisations qui permettent aux administrateurs principaux d'exécuter le runbook AWSQuickSetupType-EnableDHMC Automation, qui active la configuration de gestion des hôtes par défaut.

AWSQuickSetupEnableDHMCExecutionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSetupEnableDHMCExecutionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 novembre 2024, 21:27 UTC
- Heure modifiée : 15 novembre 2024, 21:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupEnableDHMCExecutionPolicy

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSetupJITNADeploymentRolePolicy

Description : Cette politique permet à Quick Setup de déployer le type de configuration requis pour configurer l'accès juste à temps aux nœuds.

AWSQuickSetupJITNADeploymentRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSetupJITNADeploymentRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 avril 2025, 09:07 UTC
- Heure modifiée : 07 septembre 2026, 12:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupJITNADeploymentRolePolicy

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
            ]
        }
    }
}
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSetupManagedInstanceProfileExecutionPolicy

Description : Cette politique accorde des autorisations administratives qui permettent à Systems Manager de créer un profil d'instance IAM par défaut pour la fonctionnalité de configuration rapide et de l'associer aux instances Amazon EC2 auxquelles aucun profil d'instance n'est encore associé.

AWSQuickSetupManagedInstanceProfileExecutionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSetupManagedInstanceProfileExecutionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 novembre 2024, 21:51 UTC
- Heure modifiée : 03 juin 2026, 14:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupManagedInstanceProfileExecutionPolicy`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            ]
        }
    }
}
]
}
}
}
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSetupManageJITNAResourcesExecutionPolicy

Description : Cette politique fournit des autorisations permettant d'activer l'accès juste à temps aux nœuds pour Systems Manager.

AWSQuickSetupManageJITNAResourcesExecutionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSetupManageJITNAResourcesExecutionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 avril 2025, 21:37 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupManageJITNAResourcesExecutionPolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSetupPatchPolicyBaselineAccess

Description : fournit des autorisations en lecture seule pour accéder aux bases de référence des correctifs qui ont été configurées par un administrateur de l'organisation actuelle Compte AWS à l'aide de la configuration rapide.

AWSQuickSetupPatchPolicyBaselineAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSetupPatchPolicyBaselineAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 juin 2024, 09:38 UTC
- Heure modifiée : 26 juin 2024, 09:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
            ]
        }
    }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSetupPatchPolicyDeploymentRolePolicy

Description : fournit des autorisations qui permettent à Quick Setup de créer des ressources associées à la configuration d'une politique de correctifs.

AWSQuickSetupPatchPolicyDeploymentRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSetupPatchPolicyDeploymentRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 juin 2024, 09:57 UTC
- Heure modifiée : 04 septembre 2026, 08:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyDeploymentRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
                ]
            }
        }
    }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSetupPatchPolicyLambdaExecutionPolicy

Description : accorde les autorisations nécessaires pour gérer les associations de State Manager pour les opérations de nettoyage automatisées lorsque les configurations Quick Setup sont supprimées.

AWSQuickSetupPatchPolicyLambdaExecutionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSetupPatchPolicyLambdaExecutionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 juin 2026, 14:12 UTC
- Heure modifiée : 03 juin 2026, 14:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyLambdaExecutionPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSetupPatchPolicyPermissionsBoundary

Description : QuickSetup crée des rôles IAM qui lui permettent de configurer la fonctionnalité de gestionnaire de correctifs de Systems Manager en votre nom, et utilise cette politique lors de la création de tels rôles pour définir la limite de leurs autorisations.

AWSQuickSetupPatchPolicyPermissionsBoundary est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSQuickSetupPatchPolicyPermissionsBoundary` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 juin 2024, 09:46 UTC
- Heure modifiée : 05 mars 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyPermissionsBoundary`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSetupPatchPolicyTagManagementExecutionPolicy

Description : accorde les autorisations nécessaires pour suivre les instances gérées par les configurations de politique de correctifs de Quick Setup grâce à un balisage automatique et à une collecte d'inventaire.

AWSQuickSetupPatchPolicyTagManagementExecutionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSetupPatchPolicyTagManagementExecutionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 juin 2026, 14:12 UTC
- Heure modifiée : 03 juin 2026, 14:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyTagManagementExecutionPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSetupSchedulerPermissionsBoundary

Description : La AWSQuickSetupSchedulerPermissionsBoundary politique définit la liste des autorisations autorisées dans un rôle IAM créé par Quick Setup. La configuration rapide utilise un rôle créé avec cette politique pour activer et configurer les opérations planifiées sur les instances Amazon EC2 et d'autres ressources.

AWSQuickSetupSchedulerPermissionsBoundary est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSetupSchedulerPermissionsBoundary à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 juin 2024, 09:53 UTC
- Heure modifiée : 26 juin 2024, 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSchedulerPermissionsBoundary`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSetupSSMDeploymentRolePolicy

Description : Cette politique accorde des autorisations administratives qui permettent à Quick Setup de créer des ressources qui sont utilisées lors du processus d'intégration de Systems Manager.

AWSQuickSetupSSMDeploymentRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSetupSSMDeploymentRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 novembre 2024, 22:53 UTC
- Heure modifiée : 07 septembre 2026, 12:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMDeploymentRolePolicy`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            ]
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSetupSSMDeploymentS3BucketRolePolicy

Description : Cette politique accorde des autorisations pour répertorier tous les compartiments S3 d'un compte et pour gérer et récupérer des informations sur des compartiments spécifiques du compte principal qui sont gérés via des modèles. AWS CloudFormation

AWSQuickSetupSSMDeploymentS3BucketRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSetupSSMDeploymentS3BucketRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 novembre 2024, 22:01 UTC
- Heure modifiée : 15 novembre 2024, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMDeploymentS3BucketRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSetupSSMHostMgmtPermissionsBoundary

Description : Quick Setup crée des rôles IAM qui lui permettent de configurer le type de configuration rapide Host Manager en votre nom, et utilise cette politique lors de la création de tels rôles pour définir la limite de leurs autorisations.

AWSQuickSetupSSMHostMgmtPermissionsBoundary est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSetupSSMHostMgmtPermissionsBoundary à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 juin 2024, 09:48 UTC
- Heure modifiée : 26 juin 2024, 09:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMHostMgmtPermissionsBoundary`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      ]
    }
  ]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSetupSSMLifecycleManagementExecutionPolicy

Description : La politique accorde des autorisations administratives qui permettent à Quick Setup d'exécuter une ressource AWS CloudFormation personnalisée sur les événements du cycle de vie lors du déploiement de Quick Setup dans Systems Manager.

AWSQuickSetupSSMLifecycleManagementExecutionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSQuickSetupSSMLifecycleManagementExecutionPolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 novembre 2024, 21:55 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMLifecycleManagementExecutionPolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSetupSSMManageResourcesExecutionPolicy

Description : Cette politique accorde des autorisations qui permettent à Systems Manager de créer des prérequis tels que les rôles IAM requis pour l'intégration de Systems Manager.

AWSQuickSetupSSMManageResourcesExecutionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSetupSSMManageResourcesExecutionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 novembre 2024, 22:49 UTC
- Heure modifiée : 15 novembre 2024, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMManageResourcesExecutionPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-ManagedInstanceProfile*"
},
{
    "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}"
      ]
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSetupStartSSMAssociationsExecutionPolicy

Description : Cette politique accorde des autorisations qui permettent aux administrateurs d'exécuter le runbook AWSQuickSetupType-StartSSMAssociations Automation, qui démarre State Manager Associations.

AWSQuickSetupStartSSMAssociationsExecutionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSetupStartSSMAssociationsExecutionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 août 2025, 12:04 UTC
- Heure modifiée : 05 mars 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupStartSSMAssociationsExecutionPolicy`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
      ]
    }
  }
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSetupStartStopInstancesExecutionPolicy

Description : La politique gérée AWSQuickSetupStartStopInstancesExecutionPolicy fournit des autorisations permettant à Quick Setup de démarrer et d'arrêter les instances Amazon EC2 selon un calendrier. Cette politique est utilisée avec le type de configuration du planificateur Quick Setup.

AWSQuickSetupStartStopInstancesExecutionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSetupStartStopInstancesExecutionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 août 2025, 12:04 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupStartStopInstancesExecutionPolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
        ]
    }
}
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSightAssetBundleExportPolicy

Description : fournit l'ensemble des autorisations requises pour effectuer des opérations d'exportation d'ensembles d' QuickSight actifs

AWSQuickSightAssetBundleExportPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSightAssetBundleExportPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 mars 2024, 21:31 UTC
- Heure modifiée : 27 mars 2024, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightAssetBundleExportPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
}
]
}

```


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSightAssetBundleImportPolicy

Description : fournit l'ensemble des autorisations requises pour effectuer des opérations d'importation de groupes d' QuickSight actifs

AWSQuickSightAssetBundleImportPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSightAssetBundleImportPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 mars 2024, 21:40 UTC
- Heure modifiée : 27 mars 2024, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightAssetBundleImportPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*:*:vpccconnection/*"
  },
  {
    "Sid" : "AssetBundleImportOperations",
    "Effect" : "Allow",
    "Action" : [
      "quicksight:DescribeAssetBundleImportJob",
      "quicksight:ListAssetBundleImportJobs",
      "quicksight:StartAssetBundleImportJob"
    ],
    "Resource" : "arn:aws:quicksight:*:*:asset-bundle-import-job/*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuicksightAthenaAccess

Description : Accès rapide à l'API Athena et aux compartiments S3 utilisés pour les résultats des requêtes Athena

AWSQuicksightAthenaAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuicksightAthenaAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 09 décembre 2016, 02:31 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess`

Version de la politique

Version de la politique : v13 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "*"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSightDescribeRDS

Description : Permet QuickSight de décrire les ressources RDS

AWSQuickSightDescribeRDSe est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSightDescribeRDS à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 10 novembre 2015, 23:24 UTC
- Heure modifiée : 10 novembre 2015, 23:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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



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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSightDescribeRedshift

Description : Autoriser QuickSight à décrire les ressources Redshift

AWSQuickSightDescribeRedshift est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSightDescribeRedshift à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 10 novembre 2015, 23:25 UTC
- Heure modifiée : 10 novembre 2015, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSightElasticsearchPolicy

Description : Permet d'accéder aux ressources Amazon Elasticsearch depuis Amazon QuickSight

AWSQuickSightElasticsearchPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSightElasticsearchPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 09 septembre 2020, 17:27 UTC
- Heure modifiée : 07 septembre 2021, 23:25 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSightIoTAnalyticsAccess

Description : Donnez un accès QuickSight en lecture seule aux ensembles de données IoT Analytics

AWSQuickSightIoTAnalyticsAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSightIoTAnalyticsAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2017, 17:00 UTC
- Heure modifiée : 29 novembre 2017, 17:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSightListIAM

Description : QuickSight Autoriser la liste des entités IAM

AWSQuickSightListIAMest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSQuickSightListIAM` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 10 novembre 2015, 23:25 UTC
- Heure modifiée : 10 novembre 2015, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuicksightOpenSearchPolicy

Description : Permet d'accéder aux OpenSearch ressources Amazon depuis Amazon QuickSight

AWSQuicksightOpenSearchPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuicksightOpenSearchPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 07 septembre 2021, 23:26 UTC
- Heure modifiée : 07 septembre 2021, 23:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSightSageMakerPolicy

Description : Permet d'accéder aux SageMaker ressources Amazon depuis Amazon QuickSight

AWSQuickSightSageMakerPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSightSageMakerPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 17 janvier 2020, 17:18 UTC
- Heure modifiée : 30 octobre 2023, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
    }
  ]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSightSecretsManagerWriteAccess

Description : Politique utilisée QuickSight pour créer des secrets dans AWS Secrets Manager et pour associer des politiques de ressources aux QuickSight secrets existants.

AWSQuickSightSecretsManagerWriteAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSightSecretsManagerWriteAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 22 mai 2025, 01:22 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSecretsManagerWriteAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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!*"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSightSecretsManagerWritePolicy

Description : Politique utilisée QuickSight pour créer des secrets dans AWS Secrets Manager et pour associer des politiques de ressources aux QuickSight secrets existants.

AWSQuickSightSecretsManagerWritePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSightSecretsManagerWritePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 mai 2025, 19:22 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightSecretsManagerWritePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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!*"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSQuickSightTimestreamPolicy

Description : AWS QuickSight accès aux API AWS Timestream. Les clients peuvent associer cette politique au AWS QuickSight rôle pour permettre la récupération des données et des métadonnées.

AWSQuickSightTimestreamPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSQuickSightTimestreamPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 30 septembre 2020, 21:47 UTC

- Heure modifiée : 30 septembre 2020, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSReachabilityAnalyzerServiceRolePolicy

Description : permet à VPC Reachability Analyzer d'accéder aux AWS ressources et de s'intégrer aux AWS organisations en votre nom.

AWSReachabilityAnalyzerServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 23 novembre 2022, 17:12 UTC
- Heure modifiée : 14 août 2026, 17:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  ]
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSRefactoringToolkitFullAccess

Description : Cette politique autorise l'utilisation de AWS services avec l'extension AWS Toolkit for .NET Refactoring pour Microsoft Visual Studio. Il est destiné à être rattaché à un AWS profil local. La politique permet de charger des artefacts d'application et de télécharger les artefacts qui en résultent depuis Amazon S3. Il permet de créer des applications dans une image de conteneur en utilisant, en stockant AWS CodeBuild et en récupérant les images depuis Amazon Elastic Container Registry (Amazon ECR). Il permet également le déploiement de l'application sur des services de conteneurs AWS tels qu'Amazon Elastic Container Service (Amazon ECS), la création facultative de ressources VPC, la connexion facultative à une infrastructure existante telle que AWS Directory Service, et d'autres services connexes.

AWSRefactoringToolkitFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSRefactoringToolkitFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 octobre 2022, 16:41 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSRefactoringToolkitSidecarPolicy

Description : Cette politique est destinée à être utilisée par Amazon ECS Tasks créées pour tester les applications AWS utilisant l'extension AWS Toolkit for .NET Refactoring pour Microsoft Visual Studio. La politique autorise l'accès au téléchargement d'artefacts d'application depuis Amazon S3, à la communication de l'état de la tâche à l'aide de AWS Systems Manager et à d'autres services requis.

AWSRefactoringToolkitSidecarPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSRefactoringToolkitSidecarPolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 octobre 2022, 16:41 UTC
- Heure modifiée : 29 octobre 2022, 22:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSrePostPrivateCloudWatchAccess

Description : Fournit un accès privé à Re:Post pour publier des données de métriques CloudWatch

AWSrePostPrivateCloudWatchAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 15 novembre 2023, 16:37 UTC
- Heure modifiée : 15 novembre 2023, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSrePostPrivateCloudWatchAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSRepostSpaceSupportOperationsPolicy

Description : Cette politique permet au service Re:POST Space de créer, de gérer et de résoudre les demandes de support créées via l'application Space.

AWSRepostSpaceSupportOperationsPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSRepostSpaceSupportOperationsPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 novembre 2023 à 21:52 UTC
- Heure modifiée : 26 novembre 2023, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
{
  "Sid" : "RepostSpaceSupportOperations",
  "Effect" : "Allow",
  "Action" : [
    "support:AddAttachmentsToSet",
    "support:AddCommunicationToCase",
    "support:CreateCase",
    "support:DescribeCases",
    "support:DescribeCommunications",
    "support:ResolveCase"
  ],
  "Resource" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSResilienceHubAssessmentExecutionPolicy

Description : Politique pour le rôle de service AWS Resilience Hub qui permet d'accéder à d'autres AWS services afin d'exécuter une évaluation.

AWSResilienceHubAssessmentExecutionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSResilienceHubAssessmentExecutionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 juin 2023, 12:32 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC

- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubAssessmentExecutionPolicy`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSResilienceHubResilienceTestingPolicy

Description : Politique pour le rôle de service AWS Resilience Hub qui permet d'accéder au service AWS Fault Injection afin de démarrer les tests de résilience.

AWSResilienceHubResilienceTestingPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSResilienceHubResilienceTestingPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 31 juillet 2026, 22:27 UTC
- Heure modifiée : 31 juillet 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubResilienceTestingPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSResilienceHubServiceRolePolicy

Description : permet à AWS Resilience Hub d'accéder aux ressources de votre compte pour la découverte, l'évaluation et la gestion de la résilience.

AWSResilienceHubServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 28 mai 2026, 17:42 UTC
- Heure modifiée : 06 juillet 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResilienceHubServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSResilienceHubV2AssessmentExecutionPolicy

Description : permet à AWS Resilience Hub d'accéder aux ressources de votre compte pour la découverte, l'évaluation et la gestion de la résilience. Cette politique accorde des autorisations de lecture seule avec caractères génériques qui peuvent inclure des informations sensibles dans la sortie.

AWSResilienceHubV2AssessmentExecutionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSResilienceHubV2AssessmentExecutionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 juin 2026, 22:57 UTC
- Heure modifiée : 17 juin 2026, 22:57 UTC

- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubV2AssessmentExecutionPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*",
"dsq1:Get*",
"dsq1: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*",
"qlldb:Describe*",
"qlldb: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}"
        }
    }
}

```

```
}  
  }  
    }  
      ]  
    }  
  }
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSResourceAccessManagerFullAccess

Description : fournit un accès complet au gestionnaire d'accès aux AWS ressources

AWSResourceAccessManagerFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSResourceAccessManagerFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 juin 2019, 17:28 UTC
- Heure modifiée : 04 juin 2019, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSResourceAccessManagerReadOnlyAccess

Description : fournit un accès en lecture seule au AWS Resource Access Manager.

AWSResourceAccessManagerReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSResourceAccessManagerReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 décembre 2019, 20:58 UTC
- Heure modifiée : 09 décembre 2019, 20:58 UTC

- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSResourceAccessManagerResourceShareParticipantAccess

Description : Permet d'accéder aux API AWS Resource Access Manager nécessaires à un participant au partage de ressources.

AWSResourceAccessManagerResourceShareParticipantAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSResourceAccessManagerResourceShareParticipantAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 décembre 2019, 20:41 UTC
- Heure modifiée : 09 décembre 2019, 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerResourceShareParticipantAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSResourceAccessManagerServiceRolePolicy

Description : Politique contenant l'accès du gestionnaire d'accès aux Read-only AWS ressources à la structure des organisations des clients. Il contient également des autorisations IAM pour supprimer le rôle.

AWSResourceAccessManagerServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 14 novembre 2018, 19:28 UTC
- Heure modifiée : 14 novembre 2018, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSResourceExplorerFullAccess

Description : Cette politique accorde des autorisations administratives pour accéder aux ressources de l'Explorateur de ressources et accorde des autorisations en lecture seule aux autres AWS services pour prendre en charge cet accès.

AWSResourceExplorerFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSResourceExplorerFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 novembre 2022, 20:01 UTC
- Heure modifiée : 14 novembre 2023, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            ]
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSResourceExplorerOrganizationsAccess

Description : Cette politique accorde des autorisations administratives à Resource Explorer et accorde des autorisations en lecture seule aux autres AWS services pour prendre en charge cet accès. L'administrateur AWS des organisations a besoin de ces autorisations pour configurer et gérer la recherche multicompte dans la console.

AWSResourceExplorerOrganizationsAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSResourceExplorerOrganizationsAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 novembre 2023, 17:01 UTC
- Heure modifiée : 14 novembre 2023, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
}
```

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSResourceExplorerReadOnlyAccess

Description : Cette politique accorde des autorisations en lecture seule pour rechercher et afficher les ressources de l'Explorateur de ressources et accorde des autorisations en lecture seule aux autres AWS services pour prendre en charge cet accès.

AWSResourceExplorerReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSResourceExplorerReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 novembre 2022, 19:56 UTC
- Heure modifiée : 14 novembre 2023, 16:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSResourceExplorerServiceRolePolicy

Description : permet à l'Explorateur de ressources d'afficher les ressources et les CloudTrail événements en votre nom afin d'indexer vos ressources à des fins de recherche.

AWSResourceExplorerServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 25 octobre 2022, 20:35 UTC
- Heure modifiée : 01 octobre 2026, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy`

Version de la politique

Version de la politique : v56 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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",
"dsq1:GetCluster",
"dsq1:GetClusterPolicy",
"dsq1:GetVpcEndpointServiceName",
"dsq1:ListClusters",
"dsq1: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",
"finespace: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",
```



```
"resiliencyhub: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:DescribeVPCCConnection",
"quicksight:ListAnalyses",
"quicksight:ListCustomPermissions",
"quicksight:ListDashboards",
"quicksight:ListOAuthClientApplications",
"quicksight:ListRefreshSchedules",
"quicksight:ListTagsForResource",
"quicksight:ListTopics",
"quicksight:ListVPCCConnections",
"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:GetNamespaces",
"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:DescribeSenderId",
"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",
"texttract:GetAdapter",
"texttract:ListAdapters",
"texttract: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" : "*"
}
]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSResourceGroupsReadOnlyAccess

Description : Il s'agit de la politique en lecture seule pour les groupes AWS de ressources

AWSResourceGroupsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSResourceGroupsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 mars 2018, 10:27 UTC

- Heure modifiée : 05 février 2019, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSRevenueAttributionManagement

Description : fournit l'accès nécessaire aux activités de gestion de l'attribution des recettes.

AWSRevenueAttributionManagement est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSRevenueAttributionManagement` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 juin 2026, 16:57 UTC
- Heure modifiée : 30 juin 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRevenueAttributionManagement`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ]
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSRoboMaker_FullAccess

Description : fournit un accès complet AWS RoboMaker via le SDK Console de gestion AWS et. Fournit également un accès sélectif à des services connexes (par exemple, S3, IAM).

AWSRoboMaker_FullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSRoboMaker_FullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 10 septembre 2020, 18:34 UTC
- Heure modifiée : 16 septembre 2021, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            }
        }
    }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSRoboMakerReadOnlyAccess

Description : fournit un accès en lecture seule AWS RoboMaker via le SDK Console de gestion AWS et

AWSRoboMakerReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSRoboMakerReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 26 novembre 2018, 05:30 UTC
- Heure modifiée : 28 août 2020, 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSRoboMakerServicePolicy

Description : politique RoboMaker de service

AWSRoboMakerServicePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 26 novembre 2018, 06:30 UTC
- Heure modifiée : 11 novembre 2021, 22:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"  
    ]  
  }  
}  
]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSRoboMakerServiceRolePolicy

Description : politique RoboMaker de service

AWSRoboMakerServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSRoboMakerServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 novembre 2018, 05:33 UTC
- Heure modifiée : 26 novembre 2018, 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSRolesAnywhereFullAccess

Description : fournit toutes les autorisations aux ressources IAM Roles Anywhere, y compris, mais sans s'y limiter : CreateProfile,, DisableCrl DeleteTrustAnchor,, ResetNotificationSettings

AWSRolesAnywhereFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSRolesAnywhereFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 16 juillet 2025, 14:52 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: arn:aws:iam::aws:policy/AWSRolesAnywhereFullAccess

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSRolesAnywhereReadOnly

Description : fournit des autorisations en lecture seule aux ressources IAM Roles Anywhere, y compris, mais sans s'y limiter, : GetTrustAnchor, ListProfiles GetCRL. Il n'y aura aucune autre autorisation pour les autres services inclus dans cette politique.

AWSRolesAnywhereReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSRolesAnywhereReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 16 juillet 2025, 15:07 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRolesAnywhereReadOnly`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
      "*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSRolesAnywhereServicePolicy

Description : permet à IAM Roles Anywhere de publier service/usage des métriques CloudWatch et de vérifier le statut des autorités de certification privées en votre nom.

AWSRolesAnywhereServicePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 05 juillet 2022, 15:26 UTC
- Heure modifiée : 05 juillet 2022, 15:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*:*:*"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSS3OnOutpostsServiceRolePolicy

Description : Autorisez le service Amazon S3 on Outposts à gérer les ressources réseau EC2 en votre nom.

AWSS3OnOutpostsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 03 octobre 2023, 20:32 UTC
- Heure modifiée : 03 octobre 2023, 20:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSS3OutpostsServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSavingsPlansFullAccess

Description : Fournit un accès complet au service des plans d'épargne

AWSSavingsPlansFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSavingsPlansFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 novembre 2019, 22:45 UTC
- Heure modifiée : 06 novembre 2019, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
    "Action" : "savingsplans:*",
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSavingsPlansReadOnlyAccess

Description : Fournit un accès en lecture seule au service Savings Plans

AWSSavingsPlansReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSavingsPlansReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 novembre 2019, 22:45 UTC
- Heure modifiée : 06 novembre 2019, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSDMPServiceRolePolicy

Description : Autorisez SDMP à créer et à gérer des ressources pour le compte du client.

AWSSDMPServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 24 juillet 2026, 20:57 UTC
- Heure modifiée : 10 août 2026, 22:27 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSDMPServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWS Secrets Manager Client ReadOnly Access

Description : permet de récupérer et de décrire des secrets depuis Secrets Manager. Cette politique permet également de déchiffrer les clés KMS pour les secrets de Secrets Manager.

AWS Secrets Manager Client ReadOnly Access est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWS Secrets Manager Client ReadOnly Access à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 novembre 2025, 20:04 UTC
- Heure modifiée : 02 juin 2026, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSecretsManagerClientReadOnlyAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

```
}  
  }  
  ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSecurityAgentServiceRolePolicy

Description : permet à AWS Security Agent de gérer les ressources en votre nom.

AWSSecurityAgentServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 11 juin 2026, 23:42 UTC
- Heure modifiée : 11 juin 2026, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityAgentServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            }
        }
    }
]
}

```


En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSecurityAgentWebAppPolicy

Description : autorise les utilisateurs authentifiés à accéder à l'application Web Security Agent pour configurer et exécuter des tests d'intrusion de sécurité automatisés. Cette politique permet aux utilisateurs de gérer les pentests, de consulter les résultats, de surveiller l'exécution des tests et d'interagir avec les AWS ressources nécessaires aux opérations de tests de sécurité.

AWSecurityAgentWebAppPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSecurityAgentWebAppPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 05 février 2026, 23:19 UTC
- Heure modifiée : 24 septembre 2026, 23:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSecurityAgentWebAppPolicy`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  }
}

```

```
}  
  }  
    }  
      ]  
    }  
  }
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSecurityHubFullAccess

Description : fournit un accès complet pour utiliser AWS Security Hub.

AWSSecurityHubFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSecurityHubFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 novembre 2018, 23:54 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubFullAccess`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSecurityHubOrganizationsAccess

Description : accorde l'autorisation d'activer et de gérer AWS Security Hub au sein d'une organisation. Cela inclut l'activation du service dans l'ensemble de l'organisation et la détermination du compte administrateur délégué pour le service.

AWSSecurityHubOrganizationsAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSecurityHubOrganizationsAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 15 mars 2021, 20:53 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubOrganizationsAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSecurityHubReadOnlyAccess

Description : fournit un accès en lecture seule aux ressources AWS de Security Hub

AWSSecurityHubReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSecurityHubReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2018, 01:34 UTC
- Heure modifiée : 22 février 2024, 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubReadOnlyAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSecurityHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:Get*",
        "securityhub:List*",
        "securityhub:BatchGet*",
        "securityhub:Describe*"
      ]
    }
  ]
}
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSecurityHubServiceRolePolicy

Description : rôle lié à un service requis pour que AWS Security Hub puisse accéder à vos ressources.

AWSSecurityHubServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 27 novembre 2018, 23:47 UTC
- Heure modifiée : 27 juin 2026, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubServiceRolePolicy`

Version de la politique

Version de la politique : v16 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]

```

```
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSecurityHubV2ServiceRolePolicy

Description : Cette politique permet à Security Hub de gérer les règles de AWS configuration et les ressources Security Hub au sein de votre organisation et en votre nom.

AWSSecurityHubV2ServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 10 juin 2025, 17:37 UTC
- Heure modifiée : 27 juin 2026, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSecurityHubV2ServiceRolePolicy`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
                ]
            }
        }
    }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSecurityIncidentResponseCaseFullAccess

Description : La politique fournit aux clients des autorisations de lecture et d'écriture sur les ressources de cas créées par le biais du service de réponse aux incidents de sécurité.

AWSSecurityIncidentResponseCaseFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSecurityIncidentResponseCaseFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2024, 23:21 UTC
- Heure modifiée : 22 avril 2026, 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityIncidentResponseCaseFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSecurityIncidentResponseFullAccess

Description : La politique fournit aux clients des autorisations de lecture et d'écriture sur toutes les ressources associées au service de réponse aux incidents de sécurité.

AWSSecurityIncidentResponseFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSecurityIncidentResponseFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2024, 23:21 UTC
- Heure modifiée : 22 avril 2026, 16:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSecurityIncidentResponseFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSecurityIncidentResponseReadOnlyAccess

Description : La politique accorde aux clients des Read-only autorisations d'accès à toutes les ressources associées au service de réponse aux incidents de sécurité. L'autorisation inclut également l'accès `GetCaseAttachmentDownloadUrl` à la possibilité d'obtenir les URL de téléchargement des pièces jointes à un dossier.

AWSSecurityIncidentResponseReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSecurityIncidentResponseReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2024, 23:06 UTC
- Heure modifiée : 01 octobre 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityIncidentResponseReadOnlyAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSecurityIncidentResponseServiceRolePolicy

Description : Permet d'accéder aux AWS ressources gérées ou utilisées par Security Incident Response

AWSecurityIncidentResponseServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 01 décembre 2024, 16:36 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityIncidentResponseServiceRolePolicy`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
    }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSecurityIncidentResponseTriageServiceRolePolicy

Description : donne accès à AWS la réponse aux incidents de sécurité pour surveiller en permanence votre environnement pour détecter les menaces de sécurité, ajuster les services de sécurité afin de réduire le bruit des alertes et recueillir des informations pour enquêter sur les incidents potentiels.

AWSSecurityIncidentResponseTriageServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- **Type** : politique de Service-linked rôle
- **Heure de création** : 01 décembre 2024, 16:36 UTC
- **Heure modifiée** : 12 février 2026, 17:58 UTC
- **ARN**: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityIncidentResponseTriageServiceRolePolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]

```



```
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceCatalogAdminFullAccess

Description : fournit un accès complet aux fonctionnalités d'administration du catalogue de services

AWSServiceCatalogAdminFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSServiceCatalogAdminFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 février 2018, 17:19 UTC
- Heure modifiée : 04 août 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceCatalogAdminReadOnlyAccess

Description : fournit un accès en lecture seule aux fonctionnalités d'administration du catalogue de services

AWSServiceCatalogAdminReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSServiceCatalogAdminReadOnlyAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 octobre 2019, 18:53 UTC
- Heure modifiée : 25 octobre 2019, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceCatalogAppRegistryFullAccess

Description : fournit un accès complet aux fonctionnalités du registre des applications du catalogue de services

AWSServiceCatalogAppRegistryFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSServiceCatalogAppRegistryFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 novembre 2020, 22:25 UTC
- Heure modifiée : 12 août 2026, 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryFullAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*:*:*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceCatalogAppRegistryReadOnlyAccess

Description : fournit un accès en lecture seule aux fonctionnalités du registre des applications du catalogue de services

AWSServiceCatalogAppRegistryReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSServiceCatalogAppRegistryReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 novembre 2020, 22:34 UTC
- Heure modifiée : 17 novembre 2022, 18:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceCatalogAppRegistryServiceRolePolicy

Description : Permet à Service Catalog AppRegistry de gérer des groupes de ressources en votre nom

AWSServiceCatalogAppRegistryServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 18 mai 2021, 22:18 UTC
- Heure modifiée : 26 octobre 2022, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
    ]
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceCatalogEndUserFullAccess

Description : fournit un accès complet aux fonctionnalités du catalogue de services destinées aux utilisateurs finaux

AWSServiceCatalogEndUserFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSServiceCatalogEndUserFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 février 2018, 17:22 UTC
- Heure modifiée : 04 août 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceCatalogEndUserReadOnlyAccess

Description : fournit un accès en lecture seule aux fonctionnalités de Service Catalog destinées aux utilisateurs finaux

AWSServiceCatalogEndUserReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSServiceCatalogEndUserReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 octobre 2019, 18:49 UTC
- Heure modifiée : 25 octobre 2019, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceCatalogOrgsDataSyncServiceRolePolicy

Description : Une politique de rôle liée aux services AWS ServiceCatalog pour la synchronisation avec la structure organisationnelle AWS des organisations

AWSServiceCatalogOrgsDataSyncServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 10 avril 2023, 20:48 UTC

- Heure modifiée : 08 décembre 2025, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
      }
    }
  ]
}
```

```
}  
  }  
  ]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceCatalogSyncServiceRolePolicy

Description : Un rôle lié à un service pour synchroniser les artefacts de provisionnement AWS ServiceCatalog à partir des référentiels sources

AWSServiceCatalogSyncServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 15 novembre 2022, 21:20 UTC
- Heure modifiée : 03 mai 2024, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRoleForAIDevOpsPolicy

Description : Ce rôle lié à un service AIDevOps permet de fournir des informations d'utilisation.

AWSServiceRoleForAIDevOpsPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 16 février 2026, 14:27 UTC
- Heure modifiée : 27 mars 2026, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAIDevOpsPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
}

```

```
]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRoleForAmazonEKSNodegroup

Description : autorisations requises pour gérer les groupes de nœuds dans le compte du client. Ces politiques concernaient la gestion des ressources suivantes : AutoScalingGroups SecurityGroups, LaunchTemplates et InstanceProfiles.

AWSServiceRoleForAmazonEKSNodegroup est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 07 novembre 2019, 01:34 UTC
- Heure modifiée : 17 février 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup`

Version de la politique

Version de la politique : v11 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
      ]
    }
  }
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRoleForAmazonQDeveloper

Description : Ce rôle lié à un service permet à Amazon Q Developer de fournir des informations d'utilisation.

AWSServiceRoleForAmazonQDeveloper est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 25 avril 2024, 07:40 UTC
- Heure modifiée : 20 juillet 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonQDeveloper`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRoleForAWSTransform

Description : Ce Service-Linked rôle permet à AWS Transform de fournir des informations d'utilisation.

AWSServiceRoleForAWSTransform est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 15 mai 2025, 13:37 UTC
- Heure modifiée : 12 février 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAWSTransform`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
  }
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRoleForAWSTransformCustom

Description : permet à AWS Transform Custom de publier CloudWatch des statistiques sur votre compte en votre nom.

AWSServiceRoleForAWSTransformCustom est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 25 mars 2026, 02:57 UTC
- Heure modifiée : 05 mai 2026, 19:42 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAWSTransformCustom

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
      }
    }
  ]
}
```

```
]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

Description : Permet d'accéder aux ressources de Systems Manager utilisées par CloudWatch les alarmes

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 01 octobre 2020, 09:49 UTC
- Heure modifiée : 01 octobre 2020, 09:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy

Description : Permet d'accéder CloudWatch aux statistiques de RDS Performance Insights en votre nom

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 07 septembre 2023, 09:32 UTC
- Heure modifiée : 07 septembre 2023, 09:32 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRoleForCodeGuru-Profiler

Description : rôle lié à un service requis pour qu'Amazon CodeGuru Profiler puisse envoyer des notifications en votre nom.

AWSServiceRoleForCodeGuru-Profiler est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 26 juin 2020, 22:04 UTC
- Heure modifiée : 26 juin 2020, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuru-Profiler`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
        "sns:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRoleForCodeWhispererPolicy

Description : Ce rôle autorise l'accès CodeWhisperer aux données de votre compte pour calculer la facturation, permet de créer et d'accéder à des rapports de sécurité sur Amazon CodeGuru, et d'émettre des données à CloudWatch.

AWSServiceRoleForCodeWhispererPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 24 mars 2023, 19:39 UTC
- Heure modifiée : 09 avril 2026, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRoleForEC2ScheduledInstances

Description : Permet aux instances planifiées EC2 de lancer et de gérer des instances ponctuelles.

AWSServiceRoleForEC2ScheduledInstances est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 12 octobre 2017, 18:31 UTC
- Heure modifiée : 12 octobre 2017, 18:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
}
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

Description : AWS GroundStation utilise ce rôle lié à un service pour invoquer EC2 afin de rechercher des adresses IPv4 publiques

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 13 décembre 2022, 23:52 UTC
- Heure modifiée : 13 décembre 2022, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRoleForImageBuilder

Description : Permet EC2ImageBuilder d'appeler AWS les services en votre nom.

AWSServiceRoleForImageBuilder est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 29 novembre 2019, 22:02 UTC
- Heure modifiée : 09 juillet 2026, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForImageBuilder`

Version de la politique

Version de la politique : v28 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
      }
    }
  ]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRoleForIoTSiteWise

Description : Permet SiteWise à AWS IoT de fournir et de gérer des passerelles ainsi que d'interroger des données. La politique inclut les autorisations AWS Greengrass requises pour le déploiement vers des groupes, les autorisations AWS Lambda pour la création et la mise à jour de fonctions préfixées par un service et les autorisations AWS IoT Analytics pour interroger les données des banques de données.

AWSServiceRoleForIoTSiteWise est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 14 novembre 2018, 19:19 UTC
- Heure modifiée : 13 novembre 2023, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRoleForLogDeliveryPolicy

Description : permet au service Log Delivery de fournir des journaux en appelant Log Destination en votre nom.

AWSServiceRoleForLogDeliveryPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 04 octobre 2019, 17:31 UTC
- Heure modifiée : 15 mai 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRoleForMonitronPolicy

Description : accorde à Amazon Monitron les autorisations nécessaires pour gérer les AWS ressources, y compris l'attribution d'utilisateurs AWS SSO en votre nom.

AWSServiceRoleForMonitronPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle

- Heure de création : 02 décembre 2020, 19:06 UTC
- Heure modifiée : 07 janvier 2026, 09:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRoleForNeptuneGraphPolicy

Description : fournit un accès Cloudwatch pour publier des statistiques et des journaux opérationnels et d'utilisation pour Amazon Neptune

AWSServiceRoleForNeptuneGraphPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 29 novembre 2023, 14:03 UTC
- Heure modifiée : 29 novembre 2023, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRoleForPrivateMarketplaceAdminPolicy

Description : fournit les autorisations nécessaires pour décrire et mettre à jour les ressources du marché privé et décrire AWS les organisations

AWSServiceRoleForPrivateMarketplaceAdminPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 14 février 2024, 22:28 UTC
- Heure modifiée : 14 février 2024, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForPrivateMarketplaceAdminPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
  "*"
]
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRoleForProcurementInsightsPolicy

Description : Politique relative à Procurement Insights visant à obtenir les détails du compte de l'organisation

AWSServiceRoleForProcurementInsightsPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 03 octobre 2024, 14:26 UTC
- Heure modifiée : 03 octobre 2024, 14:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForProcurementInsightsPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProcurementInsightsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRoleForSMS

Description : donne accès aux AWS services et aux ressources nécessaires à la migration des instances de service vers EC2, S3 et Cloudformation, AWS notamment.

AWSServiceRoleForSMSe est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 06 août 2019, 18:39 UTC
- Heure modifiée : 15 octobre 2020, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRoleForUserSubscriptions

Description : permet d'accéder au service d'abonnements utilisateur à vos ressources Identity Center afin de mettre à jour automatiquement vos abonnements.

AWSServiceRoleForUserSubscription est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 25 avril 2024, 16:14 UTC
- Heure modifiée : 22 juin 2026, 08:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForUserSubscriptions`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRolePolicyForBackupReports

Description : Fournit des autorisations de AWS sauvegarde pour créer des rapports de conformité en votre nom

AWSServiceRolePolicyForBackupReportsest une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle

- Heure de création : 19 août 2021, 21:16 UTC
- Heure modifiée : 10 mars 2023, 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRolePolicyForBackupRestoreTesting

Description : Cette politique contient des autorisations permettant de tester les restaurations et de nettoyer les ressources créées lors des tests.

AWSServiceRolePolicyForBackupRestoreTesting est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 10 novembre 2023, 23:37 UTC
- Heure modifiée : 25 septembre 2026, 01:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"  
    }  
  ]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSServiceRolePolicyForWorkspacesInstances

Description : Cette politique gérée fournit un accès administratif à Amazon WorkSpaces pour gérer les instances EC2 dans votre Compte AWS

AWSServiceRolePolicyForWorkspacesInstances est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 11 juin 2025, 20:37 UTC
- Heure modifiée : 27 août 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForWorkspacesInstances`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSShieldDRTAccessPolicy

Description : fournit à l'équipe d'intervention AWS DDoS un accès limité à vous pour vous aider Compte AWS à atténuer les attaques DDoS lors d'un événement de haute gravité.

AWSShieldDRTAccessPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSShieldDRTAccessPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 05 juin 2018, 22:29 UTC
- Heure modifiée : 15 décembre 2020, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSShieldServiceRolePolicy

Description : permet à AWS Shield d'accéder aux AWS ressources en votre nom afin de fournir une protection contre les attaques DDoS.

AWSShieldServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 17 novembre 2021, 19:17 UTC
- Heure modifiée : 17 novembre 2021, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSShield",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:UpdateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSocialMessagingServiceRolePolicy

Description : permet de publier des statistiques et de fournir des informations sur l'envoi de vos messages sur les réseaux sociaux.

AWSSocialMessagingServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 10 octobre 2024, 19:28 UTC
- Heure modifiée : 10 octobre 2024, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSocialMessagingServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
```

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSSMForSAPServiceLinkedRolePolicy

Description : fournit à AWS Systems Manager pour SAP les autorisations nécessaires pour gérer et intégrer le logiciel SAP AWS.

AWSSSMForSAPServiceLinkedRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 16 novembre 2022, 01:18 UTC
- Heure modifiée : 12 février 2026, 18:03 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy`

Version de la politique

Version de la politique : v21 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSSMOpsInsightsServiceRolePolicy

Description : Politique relative au rôle lié aux services AWSServiceRoleForAmazonSSM _OpsInsights

AWSSSM0psInsightsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 16 juin 2021, 20:12 UTC
- Heure modifiée : 16 juin 2021, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSM0psInsightsServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  }
}
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSSODirectoryAdministrator

Description : Accès administrateur pour le répertoire SSO

AWSSSODirectoryAdministratorest une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSSODirectoryAdministrator à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 31 octobre 2018, 23:54 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSSODirectoryReadOnly

Description : ReadOnly accès à l'annuaire SSO

AWSSSODirectoryReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSSODirectoryReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 31 octobre 2018, 23:49 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSSOMasterAccountAdministrator

Description : Fournit un accès via AWS SSO pour gérer les comptes principaux et membres des AWS organisations ainsi que l'application cloud

AWSSSOMasterAccountAdministrator est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSSSOMasterAccountAdministrator` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 juin 2018, 20:36 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator`

Version de la politique

Version de la politique : v13 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSS0CreateSLR",
      "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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSSOMemberAccountAdministrator

Description : Fournit un accès via AWS SSO pour gérer les comptes AWS des membres des organisations et l'application cloud

AWSSSOMemberAccountAdministrator est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSSOMemberAccountAdministrator à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 juin 2018, 20:45 UTC

- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMemberAccountAdministrator`

Version de la politique

Version de la politique : v11 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSSOReadOnly

Description : fournit un accès en lecture seule aux configurations AWS SSO.

AWSSSOReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSSOReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 juin 2018, 20:24 UTC

- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSS0ReadOnly`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSS0ReadOnly",
      "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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSSOServiceRolePolicy

Description : accorde des autorisations AWS SSO pour gérer les AWS ressources, y compris les rôles IAM, les politiques et l'IdP SAML en votre nom.

AWSSSOServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 05 décembre 2017, 18:36 UTC
- Heure modifiée : 11 février 2025, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSOServiceRolePolicy`

Version de la politique

Version de la politique : v18 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  ]
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSStepFunctionsConsoleFullAccess

Description : politique d'accès pour fournir un accès user/role /etc à la AWS StepFunctions console. Pour bénéficier d'une expérience de console complète, en plus de cette politique, un utilisateur peut avoir besoin de l'PassRole autorisation iam : sur d'autres rôles IAM pouvant être assumés par le service.

AWSStepFunctionsConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSStepFunctionsConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 janvier 2017, 21:54 UTC
- Heure modifiée : 12 janvier 2017, 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSStepFunctionsFullAccess

Description : politique d'accès pour fournir un accès user/role /etc à l' AWS StepFunctions API. Pour bénéficier d'un accès complet, en plus de cette politique, un utilisateur DOIT disposer de l'PassRole autorisation iam : sur au moins un rôle IAM pouvant être assumé par le service.

AWSStepFunctionsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSStepFunctionsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 janvier 2017, 21:51 UTC
- Heure modifiée : 11 janvier 2017, 21:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSStepFunctionsReadOnlyAccess

Description : politique d'accès pour fournir un accès en lecture seule au AWS StepFunctions service user/role /etc.

AWSStepFunctionsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSStepFunctionsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 janvier 2017, 21:46 UTC
- Heure modifiée : 26 avril 2024, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSStorageGatewayFullAccess

Description : fournit un accès complet à AWS Storage Gateway via le Console de gestion AWS.

AWSStorageGatewayFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSStorageGatewayFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 06 septembre 2022, 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"  
    }  
  ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSStorageGatewayReadOnlyAccess

Description : Permet d'accéder à AWS Storage Gateway via le Console de gestion AWS.

AWSStorageGatewayReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSStorageGatewayReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 06 septembre 2022, 20:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSStorageGatewayServiceRolePolicy

Description : Service-linked rôle utilisé par AWS Storage Gateway pour permettre l'intégration d'autres AWS services à Storage Gateway.

AWSStorageGatewayServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 17 février 2021, 19:03 UTC
- Heure modifiée : 17 février 2021, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
    "Resource" : "arn:aws:fsx:*:*:backup/*"
  }
]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSupplyChainFederationAdminAccess

Description : AWSSupplyChainFederationAdminAccess permet aux utilisateurs fédérés de la chaîne d' AWS approvisionnement d'accéder à l'application AWS Supply Chain, y compris les autorisations requises pour effectuer des actions dans l'application AWS Supply Chain. La politique fournit des autorisations administratives aux utilisateurs et aux groupes d'IAM Identity Center et est associée à un rôle créé par AWS Supply Chain en votre nom. Vous ne devez pas associer AWSSupplyChainFederationAdminAccess de politique à d'autres entités IAM.

AWSSupplyChainFederationAdminAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSupplyChainFederationAdminAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 01 mars 2023, 18:54 UTC
- Heure modifiée : 14 août 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSupportAccess

Description : Permet aux utilisateurs d'accéder au AWS Support Centre.

AWSSupportAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSupportAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSupportAppFullAccess

Description : fournit un accès complet à l' AWS Support application et aux autres services requis, tels que AWS Support les quotas de service. Cette politique inclut les autorisations d'utilisation des services d'assistance afin que l'utilisateur puisse contacter AWS Support pour les demandes d'assistance, modifier les quotas de service et créer les rôles liés aux services pertinents.

AWSSupportAppFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSupportAppFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 août 2022, 16:53 UTC
- Heure modifiée : 22 août 2022, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSupportAppReadOnlyAccess

Description : fournit un accès en lecture seule à l' AWS Support application.

AWSSupportAppReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSupportAppReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 août 2022, 17:01 UTC
- Heure modifiée : 22 août 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSupportPlansFullAccess

Description : fournit un accès complet aux plans de support.

AWSSupportPlansFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSupportPlansFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 septembre 2022, 18:19 UTC
- Heure modifiée : 24 août 2026, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSupportPlansReadOnlyAccess

Description : fournit un accès en lecture seule aux plans de support.

AWSSupportPlansReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSupportPlansReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 septembre 2022, 18:08 UTC
- Heure modifiée : 24 août 2026, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:ListSupportPlanModifiers",
        "supportplans:GetSupportAgreement",
        "supportplans:ListSupportAgreements",
        "supportplans:ListSupportAgreementRevisions"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSupportPlansServiceRolePolicy

Description : permet aux AWS Support plans de lire et de mettre à jour les AWS ressources utilisées pour gérer le plan de support de votre compte en votre nom.

AWSSupportPlansServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 31 juillet 2026, 17:12 UTC
- Heure modifiée : 31 juillet 2026, 17:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSupportPlansServiceRolePolicy

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSupportServiceRolePolicy

Description : Permet d'accéder AWS Support à AWS des ressources pour fournir des services de facturation, d'administration et de support.

AWSSupportServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 19 avril 2018, 18:04 UTC
- Heure modifiée : 19 août 2026, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy`

Version de la politique

Version de la politique : v59 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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",
"dln:getLifecyclePolicies",
"dln: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",
"dms:describeJobLogItems",
"dms:describeJobs",
"dms:describeLaunchConfigurationTemplates",
"dms:describeRecoveryInstances",
"dms:describeRecoverySnapshots",
"dms:describeReplicationConfigurationTemplates",
"dms:describeSourceNetworks",
"dms:describeSourceServers",
"dms:getLaunchConfiguration",
"dms:getReplicationConfiguration",
"dms:listExtensibleSourceServers",
"dms:listLaunchActions",
"dms: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:imageBlockPublicAccessState",
"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:describeVPCCConnection",
"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:listVPCCConnections",
"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" : [
    "*"
  ]

```

```
}  
]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWS IAM Systems Manager Account Discovery Service Policy

Description : autorise le gestionnaire de AWS systèmes (SSM) à découvrir des Compte AWS informations.

AWS IAM Systems Manager Account Discovery Service Policy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 24 octobre 2019, 17:21 UTC
- Heure modifiée : 17 octobre 2022, 20:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWS IAM Systems Manager Account Discovery Service Policy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWS IAM Policy: AWSManagedServicesChangeManagementServicePolicy

Description : donne accès aux AWS ressources gérées ou utilisées par le cadre de gestion des modifications de AWS Systems Manager.

AWSManagedServicesChangeManagementServicePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 07 décembre 2020, 22:21 UTC
- Heure modifiée : 23 octobre 2025, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSystemsManagerEnableConfigRecordingExecutionPolicy

Description : fournit des autorisations permettant à AWS Systems Manager Quick Setup d'activer et de configurer l'enregistrement de la AWS configuration de configuration.

AWSSystemsManagerEnableConfigRecordingExecutionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSystemsManagerEnableConfigRecordingExecutionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 juin 2024, 09:40 UTC
- Heure modifiée : 26 juin 2024, 09:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerEnableConfigRecordingExecutionPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSystemsManagerEnableExplorerExecutionPolicy

Description : Cette politique accorde des autorisations administratives pour activer Explorer, une fonctionnalité de AWS Systems Manager. Cela inclut les autorisations nécessaires pour mettre à

jour les paramètres de service Systems Manager associés et pour créer un rôle lié à un service pour Systems Manager.

AWSSystemsManagerEnableExplorerExecutionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSystemsManagerEnableExplorerExecutionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 juin 2024, 09:42 UTC
- Heure modifiée : 26 juin 2024, 09:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSystemsManagerForSAPFullAccess

Description : fournit un accès complet au service AWS Systems Manager pour SAP

AWSSystemsManagerForSAPFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSystemsManagerForSAPFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 novembre 2022, 02:11 UTC
- Heure modifiée : 10 juillet 2024, 21:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSystemsManagerForSAPReadOnlyAccess

Description : fournit un accès en lecture seule au service AWS Systems Manager pour SAP

AWSSystemsManagerForSAPReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSystemsManagerForSAPReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 novembre 2022, 02:11 UTC
- Heure modifiée : 17 novembre 2022, 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:get*",

```

```
    "ssm-sap:list*"
  ],
  "Resource" : "arn:*:ssm-sap:*:*:*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSystemsManagerJustInTimeAccessServicePolicy

Description : Permet d'accéder aux AWS ressources gérées ou utilisées par le AWS System Manager dans le cadre d'accès juste à temps.

AWSSystemsManagerJustInTimeAccessServicePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 21 avril 2025, 20:07 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerJustInTimeAccessServicePolicy`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSystemsManagerJustInTimeAccessTokenPolicy

Description : La politique gérée AWSSystemsManagerJustInTimeAccessTokenPolicy permet à Systems Manager de générer des jetons d'accès utilisés pour l'accès aux nœuds juste à temps.

AWSSystemsManagerJustInTimeAccessTokenPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSystemsManagerJustInTimeAccessTokenPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 avril 2025, 21:07 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeAccessTokenPolicy

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSystemsManagerJustInTimeAccessTokenSessionPolicy

Description : La politique gérée AWSSystemsManagerJustInTimeAccessTokenSessionPolicy permet à Systems Manager d'appliquer des autorisations limitées à une session d'accès aux nœuds juste à temps une fois celle-ci démarrée.

AWSSystemsManagerJustInTimeAccessTokenSessionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSystemsManagerJustInTimeAccessTokenSessionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 17 avril 2025, 20:52 UTC
- Heure modifiée : 12 février 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeAccessTokenSessionPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy

Description : Cette politique permet à Systems Manager de partager une politique de refus d'accès pour l'accès juste à temps aux nœuds depuis le compte administrateur délégué vers les comptes des membres, et de répliquer la politique dans plusieurs régions.

AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 21 avril 2025, 20:52 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSystemsManagerNotificationsServicePolicy

Description : autorisations requises pour collecter des informations sur un utilisateur à Just-In-Time-Node-Access des fins de notifications.

AWSSystemsManagerNotificationsServicePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 17 avril 2025, 20:52 UTC
- Heure modifiée : 17 avril 2025, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerNotificationsServicePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
    "*"
  ]
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSSystemsManagerOpsDataSyncServiceRolePolicy

Description : rôle IAM permettant à SSM Explorer de gérer les opérations associées OpsData

AWSSystemsManagerOpsDataSyncServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 26 avril 2021, 20:42 UTC
- Heure modifiée : 28 juin 2023, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/opdata/*"
    ]
  },
  {
    "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
      }
    }
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSThinkboxAssetServerPolicy

Description : Cette politique accorde au AWS Portal Asset Server les autorisations nécessaires à un fonctionnement normal.

AWSThinkboxAssetServerPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSThinkboxAssetServerPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 mai 2020, 19:18 UTC
- Heure modifiée : 27 mai 2020, 19:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSThinkboxAWSPortalAdminPolicy

Description : Cette politique accorde au logiciel Deadline de AWS Thinkbox un accès complet à plusieurs AWS services nécessaires à l'administration AWS du portail. Cela inclut l'accès à la création de balises arbitraires sur plusieurs types de ressources EC2.

AWSThinkboxAWSPortalAdminPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSThinkboxAWSPortalAdminPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 mai 2020, 19:41 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
    }
  ]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSThinkboxAWSPortalGatewayPolicy

Description : Cette politique accorde à la machine AWS Portal Gateway les autorisations nécessaires à un fonctionnement normal.

AWSThinkboxAWSPortalGatewayPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSThinkboxAWSPortalGatewayPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 mai 2020, 19:05 UTC
- Heure modifiée : 30 juin 2020, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:rds-tls-pw-stack*"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSThinkboxAWSPortalWorkerPolicy

Description : Cette politique accorde aux Deadline Workers in AWS Portal les autorisations nécessaires à un fonctionnement normal.

AWSThinkboxAWSPortalWorkerPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSThinkboxAWSPortalWorkerPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 mai 2020, 19:15 UTC
- Heure modifiée : 07 décembre 2020, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSThinkboxDeadlineResourceTrackerAccessPolicy

Description : accorde les autorisations nécessaires au fonctionnement du Deadline Resource Tracker de AWS Thinkbox. Cela inclut un accès complet à certaines actions EC2, notamment DeleteFleets et CancelSpotFleetRequests.

AWSThinkboxDeadlineResourceTrackerAccessPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSThinkboxDeadlineResourceTrackerAccessPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 mai 2020, 19:25 UTC
- Heure modifiée : 27 mai 2020, 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAccessPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
    ]
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSThinkboxDeadlineResourceTrackerAdminPolicy

Description : accorde les autorisations nécessaires pour créer, détruire et administrer le Deadline Resource Tracker de AWS Thinkbox.

AWSThinkboxDeadlineResourceTrackerAdminPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSThinkboxDeadlineResourceTrackerAdminPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 mai 2020, 19:29 UTC
- Heure modifiée : 16 juillet 2026, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAdminPolicy`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

Description : accorde les autorisations requises pour le plug-in Deadline Spot Event de AWS Thinkbox. Cela inclut l'autorisation de demander, de modifier et d'annuler une flotte ponctuelle, ainsi qu'une PassRole autorisation limitée.

AWSThinkboxDeadlineSpotEventPluginAdminPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSThinkboxDeadlineSpotEventPluginAdminPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 mai 2020, 19:38 UTC
- Heure modifiée : 27 mai 2020, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginAdminPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

Description : accordez les autorisations requises pour une instance EC2 exécutant le logiciel AWS Thinkbox Deadline Spot Event Plugin Worker.

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSThinkboxDeadlineSpotEventPluginWorkerPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 mai 2020, 19:35 UTC
- Heure modifiée : 07 décembre 2020, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
    ]
  }
]
```

```
]
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSTransferConsoleFullAccess

Description : Fournit un accès complet à AWS Transfer via le Console de gestion AWS

AWSTransferConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSTransferConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 décembre 2020, 19:33 UTC
- Heure modifiée : 14 décembre 2020, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSTransferFullAccess

Description : Fournit un accès complet au service de AWS transfert.

AWSTransferFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSTransferFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 décembre 2020, 19:37 UTC
- Heure modifiée : 14 décembre 2020, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSTransferLoggingAccess

Description : permet de AWS transférer l'accès complet à la création de flux de journaux et de groupes et à l'ajout d'événements de journal à votre compte

AWSTransferLoggingAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSTransferLoggingAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 14 janvier 2019, 15:32 UTC
- Heure modifiée : 14 janvier 2019, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSTransferReadOnlyAccess

Description : Fournissez un accès en lecture seule aux services de AWS transfert.

AWSTransferReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSTransferReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 août 2020, 17:54 UTC
- Heure modifiée : 27 août 2020, 17:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
```

```
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSTransferServiceRolePolicy

Description : Permet à Transfer de s'intégrer à d'autres AWS services en votre nom

AWSTransferServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 22 septembre 2026, 17:07 UTC
- Heure modifiée : 22 septembre 2026, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTransferServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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
        }
    }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSTransformApplicationDeploymentPolicy

Description : permet au service AWS Transform de déployer des applications .NET transformées en créant et en gérant AWS des ressources. Cette politique accorde des autorisations pour provisionner l'infrastructure, gérer les ressources de calcul et configurer les paramètres de déploiement pour différents AWS services.

AWSTransformApplicationDeploymentPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSTransformApplicationDeploymentPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 28 août 2025, 06:34 UTC
- Heure modifiée : 11 septembre 2026, 00:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransformApplicationDeploymentPolicy`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSTransformApplicationECSDeploymentPolicy

Description : permet au AWS Transform de déployer des applications sur Amazon Elastic Container Service (ECS) avec Fargate. Il accorde les autorisations nécessaires pour provisionner, configurer et gérer l'infrastructure sous-jacente requise pour exécuter des applications sur ECS.

AWSTransformApplicationECSDeploymentPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSTransformApplicationECSDeploymentPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- **Type** : Politique relative aux rôles de service
- **Heure de création** : 29 septembre 2025, 22:49 UTC
- **Heure modifiée** : 11 septembre 2026, 00:27 UTC
- **ARN**: `arn:aws:iam::aws:policy/service-role/AWSTransformApplicationECSDeploymentPolicy`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSTransformCustomExecuteTransformations

Description : Permet d'exécuter des transformations dans AWS Transform custom.

AWSTransformCustomExecuteTransformation est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSTransformCustomExecuteTransformations à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 décembre 2025, 15:34 UTC
- Heure modifiée : 27 avril 2026, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformCustomExecuteTransformations`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSTransformCustomFullAccess

Description : fournit un accès complet à AWS Transform custom.

AWSTransformCustomFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSTransformCustomFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 décembre 2025, 15:19 UTC
- Heure modifiée : 07 avril 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformCustomFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSTransformCustomManageTransformations

Description : Permet de gérer les ressources de transformation et d'exécuter des transformations dans AWS Transform custom.

AWSTransformCustomManageTransformations est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSTransformCustomManageTransformations à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 décembre 2025, 15:49 UTC
- Heure modifiée : 27 avril 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformCustomManageTransformations`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSTransformInfrastructureExecutorAccessBatch

Description : accorde aux développeurs chargés du rôle d'exécution les autorisations nécessaires pour exécuter AWS Transform Continuous Modernization CLI/agent à assessments/transformations l'aide de AWS Batch, notamment pour le téléchargement du code source, la récupération des résultats, la surveillance de l'état des tâches Batch, la lecture des journaux et la gestion des calendriers de transformation.

AWSTransformInfrastructureExecutorAccessBatch est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSTransformInfrastructureExecutorAccessBatch à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 juillet 2026, 20:12 UTC
- Heure modifiée : 02 septembre 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformInfrastructureExecutorAccessBatch`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSTransformInfrastructureExecutorAccessEC2

Description : accorde aux développeurs chargés du rôle d'exécution les autorisations nécessaires pour exécuter AWS Transform Continuous Modernization CLI/agent à assessments/transformations l'aide d'EC2, notamment pour le téléchargement du code source, la récupération des résultats, la surveillance de l'état des tâches, la lecture des journaux et la gestion des calendriers de transformation.

AWSTransformInfrastructureExecutorAccessEC2 est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSTransformInfrastructureExecutorAccessEC2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 juillet 2026, 20:12 UTC
- Heure modifiée : 02 septembre 2026, 21:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransformInfrastructureExecutorAccessEC2

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSTransformLandingZoneAgentPolicy

Description : autorise AWS Transform à configurer des zones d' AWS atterrissage, y compris l'approvisionnement des comptes, la gouvernance organisationnelle et la configuration de la tour de contrôle

AWSTransformLandingZoneAgentPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSTransformLandingZoneAgentPolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 août 2026, 15:12 UTC
- Heure modifiée : 01 septembre 2026, 10:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformLandingZoneAgentPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
  }
}
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSTransformNetworkMigrationAgentPolicy

Description : accorde à AWS Transform l'autorisation de déployer et de configurer l'infrastructure réseau, y compris les VPC, les passerelles de transit et les tables de routage pour la migration du réseau

AWSTransformNetworkMigrationAgentPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSTransformNetworkMigrationAgentPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 août 2026, 15:27 UTC
- Heure modifiée : 01 septembre 2026, 10:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransformNetworkMigrationAgentPolicy

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  }
}

```

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSTransformRevenueAttributionPolicy

Description : permet au service AWS Transform de gérer l'attribution des revenus des clients à des fins d'incitation.

AWSTransformRevenueAttributionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSTransformRevenueAttributionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 juillet 2026, 16:42 UTC
- Heure modifiée : 07 juillet 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformRevenueAttributionPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
          ]
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSTransformSecretsManagerConnectorPolicy

Description : permet au service AWS Transform de lire un SecretsManager secret spécifié en connexion avec la clé KMS spécifiée. Cette politique accorde l'autorisation de lire la valeur secrète spécifiée et de la déchiffrer si le secret est crypté.

AWSTransformSecretsManagerConnectorPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSTransformSecretsManagerConnectorPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 mars 2026, 21:12 UTC
- Heure modifiée : 04 mars 2026, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformSecretsManagerConnectorPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSTransformSecurityAgentExecutorAccess

Description : accorde à AWS Transform (ATX) Continuous Modernization CLI/agent les autorisations nécessaires pour invoquer le service AWS Security Agent afin d'automatiser les révisions de sécurité du code et la correction, y compris le téléchargement des artefacts de numérisation et la récupération des résultats.

AWSTransformSecurityAgentExecutorAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSTransformSecurityAgentExecutorAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 juin 2026, 21:27 UTC
- Heure modifiée : 28 juillet 2026, 15:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformSecurityAgentExecutorAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSTransformServerMigrationAgentPolicy

Description : autorise AWS Transform à effectuer des opérations de migration de serveurs, notamment la réplication, les tests et le basculement à l'aide du service de migration des AWS applications

AWSTransformServerMigrationAgentPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSTransformServerMigrationAgentPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 août 2026, 15:27 UTC
- Heure modifiée : 01 septembre 2026, 10:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformServerMigrationAgentPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
    }
}
]
}
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSTrustedAdvisorPriorityFullAccess

Description : fournit un accès complet à AWS Trusted Advisor Priority. Cette politique permet également à l'utilisateur d'ajouter Trusted Advisor en tant que service sécurisé auprès AWS des organisations et de spécifier des comptes d'administrateur délégués pour Trusted Advisor Priority.

AWSTrustedAdvisorPriorityFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSTrustedAdvisorPriorityFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 16 août 2022, 16:08 UTC
- Heure modifiée : 16 août 2022, 16:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"  
  ]  
}  
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSTrustedAdvisorPriorityReadOnlyAccess

Description : fournit un accès en lecture seule à AWS Trusted Advisor Priority. Cela inclut l'autorisation de consulter les comptes d'administrateur délégués.

AWSTrustedAdvisorPriorityReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSTrustedAdvisorPriorityReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 16 août 2022, 16:35 UTC
- Heure modifiée : 16 août 2022, 16:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
          ]
        }
      }
    }
  ]
}
```

```
}  
  }  
    }  
      ]  
    }  
  }
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSTrustedAdvisorReportingServiceRolePolicy

Description : Politique de service pour les Multi-account rapports Trusted Advisor

AWSTrustedAdvisorReportingServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 19 novembre 2019, 17:41 UTC
- Heure modifiée : 28 février 2023, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSTrustedAdvisorServiceRolePolicy

Description : Accès au service AWS Trusted Advisor pour vous aider à réduire les coûts, à améliorer les performances et à renforcer la sécurité de votre AWS environnement.

AWSTrustedAdvisorServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 22 février 2018, 21:24 UTC
- Heure modifiée : 14 mai 2026, 21:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy`

Version de la politique

Version de la politique : v15 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSUserAttributeCostAllocationPolicy

Description : fournit un accès en lecture seule aux attributs utilisateur depuis AWS IAM Identity Center pour les attributs utilisateur pour lesquels le client a choisi.

AWSUserAttributeCostAllocationPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 15 décembre 2025, 16:34 UTC
- Heure modifiée : 15 décembre 2025, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserAttributeCostAllocationPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSUserNotificationsServiceLinkedRolePolicy

Description : autorise les notifications aux AWS utilisateurs à appeler AWS les services en votre nom.

AWSUserNotificationsServiceLinkedRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 19 avril 2023, 13:28 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSVendorInsightsAssessorFullAccess

Description : fournit un accès complet pour consulter les ressources Vendor Insights et gérer les abonnements Vendor Insights

AWSVendorInsightsAssessorFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSVendorInsightsAssessorFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 juillet 2022, 15:05 UTC
- Heure modifiée : 01 décembre 2022, 00:51 UTC

- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSVendorInsightsAssessorReadOnly

Description : fournit un accès en lecture seule pour consulter les ressources Vendor Insights intitulées

AWSVendorInsightsAssessorReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSVendorInsightsAssessorReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 juillet 2022, 15:05 UTC
- Heure modifiée : 01 décembre 2022, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSVendorInsightsVendorFullAccess

Description : fournit un accès complet à la création et à la gestion des ressources Vendor Insights

AWSVendorInsightsVendorFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSVendorInsightsVendorFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 juillet 2022, 15:05 UTC
- Heure modifiée : 19 octobre 2023, 01:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSVendorInsightsVendorReadOnly

Description : fournit un accès en lecture seule pour consulter les ressources Vendor Insights

AWSVendorInsightsVendorReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSVendorInsightsVendorReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 26 juillet 2022, 15:05 UTC
- Heure modifiée : 01 décembre 2022, 00:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"  
  }  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSVPCFlowLogsServiceRolePolicy

Description : fournit les autorisations nécessaires pour contrôler les ressources gérées par les services et appeler les API nécessaires à l'enrichissement des champs de journalisation pour le compte des clients.

AWSVPCFlowLogsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 11 mai 2026, 15:57 UTC
- Heure modifiée : 11 mai 2026, 15:57 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSVPCFlowLogsServiceRolePolicy

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSVpcLatticeServiceRolePolicy

Description : permet à VPC Lattice d'accéder aux AWS ressources en votre nom.

AWSVpcLatticeServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 30 novembre 2022, 20:47 UTC
- Heure modifiée : 01 décembre 2024, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]

```



```
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSVPCS2SVpnServiceRolePolicy

Description : Autorisez le Site-to-Site VPN à créer et à gérer des ressources liées à vos connexions VPN.

AWSVPCS2SVpnServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 06 août 2019, 14:13 UTC
- Heure modifiée : 15 mai 2025, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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!*"
      }
    }
  }
]
```

```
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSVPCTransitGatewayServiceRolePolicy

Description : Autorisez VPC Transit Gateway à créer et à gérer les ressources nécessaires pour vos pièces jointes VPC Transit Gateway.

AWSVPCTransitGatewayServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 26 novembre 2018, 16:21 UTC
- Heure modifiée : 15 avril 2021, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : ""
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSVPCVerifiedAccessServiceRolePolicy

Description : Politique permettant au service AWS Verified Access de provisionner des terminaux en votre nom

AWSVPCVerifiedAccessServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 29 novembre 2022, 03:35 UTC

- Heure modifiée : 17 novembre 2023, 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSWAFConsoleFullAccess

Description : Fournit un accès complet à AWS WAF via le Console de gestion AWS. Notez que cette politique accorde également des autorisations pour répertorier et mettre à jour les CloudFront distributions Amazon, des autorisations pour afficher les équilibres de charge sur AWS Elastic Load Balancing, des autorisations pour afficher les API REST et les étapes d'Amazon API Gateway, des autorisations pour répertorier et afficher CloudWatch les métriques Amazon et des autorisations pour afficher les régions activées dans le compte.

AWSWAFConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSWAFConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 avril 2020, 18:38 UTC
- Heure modifiée : 01 juillet 2026, 04:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess`

Version de la politique

Version de la politique : v22 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```

    "waf:*",
    "waf-regional:*"
  ],
  "Resource" : [
    "arn:aws:waf::*:byte-matchset/*",
    "arn:aws:waf::*:ipset/*",
    "arn:aws:waf::*:rate-based-rule/*",
    "arn:aws:waf::*:rule/*",
    "arn:aws:waf::*:size-constraint-set/*",
    "arn:aws:waf::*:sql-injection-set/*",
    "arn:aws:waf::*:web-acl/*",
    "arn:aws:waf::*:xss-matchset/*",
    "arn:aws:waf::*:regex-match/*",
    "arn:aws:waf::*:regex-pattern-set/*",
    "arn:aws:waf::*:geo-matchset/*",
    "arn:aws:waf::*:rule-group/*",
    "arn:aws:waf::*:change-token/*",
    "arn:aws:waf-regional::*:byte-matchset/*",
    "arn:aws:waf-regional::*:ipset/*",
    "arn:aws:waf-regional::*:rate-based-rule/*",
    "arn:aws:waf-regional::*:rule/*",
    "arn:aws:waf-regional::*:size-constraint-set/*",
    "arn:aws:waf-regional::*:sql-injection-set/*",
    "arn:aws:waf-regional::*:web-acl/*",
    "arn:aws:waf-regional::*:xss-matchset/*",
    "arn:aws:waf-regional::*:regex-match/*",
    "arn:aws:waf-regional::*:regex-pattern-set/*",
    "arn:aws:waf-regional::*:geo-matchset/*",
    "arn:aws:waf-regional::*:rule-group/*",
    "arn:aws:waf-regional::*:change-token/*"
  ]
},
{
  "Sid" : "AllowWAFCClassicGetWebACLForResource",
  "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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSWAFConsoleReadOnlyAccess

Description : Fournit un accès en lecture seule à AWS WAF via le. Console de gestion AWS Notez que cette politique accorde également des autorisations pour répertorier les CloudFront distributions Amazon, des autorisations pour afficher les équilibres de charge sur AWS Elastic Load Balancing, des autorisations pour afficher les API REST et les étapes d'Amazon API Gateway, des autorisations pour répertorier et afficher CloudWatch les métriques Amazon et des autorisations pour afficher les régions activées dans le compte.

AWSWAFConsoleReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSWAFConsoleReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 avril 2020, 18:43 UTC
- Heure modifiée : 01 juillet 2026, 04:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess`

Version de la politique

Version de la politique : v21 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSWAFFullAccess

Description : fournit un accès complet aux actions AWS WAF.

AWSWAFFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSWAFFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 octobre 2015, 20:44 UTC
- Heure modifiée : 28 juillet 2026, 21:42 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFFullAccess

Version de la politique

Version de la politique : v17 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "AllowWAFCClassicGetWebACLForResource",
    "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" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSWAFFReadOnlyAccess

Description : fournit un accès en lecture seule aux actions AWS WAF.

AWSWAFFReadOnlYAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSWAFFReadOnlYAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 octobre 2015, 20:43 UTC
- Heure modifiée : 01 juillet 2026, 04:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFFReadOnlYAccess`

Version de la politique

Version de la politique : v13 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSWellArchitectedAgentOrganizationsServiceRolePolicy

Description : permet à AWS Well-Architected l'agent d'accéder à la structure organisationnelle et aux informations relatives à l'administrateur délégué dans AWS les organisations en votre nom

AWSWellArchitectedAgentOrganizationsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 15 septembre 2026, 18:37 UTC
- Heure modifiée : 15 septembre 2026, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedAgentOrganizationsServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSWellArchitectedAgentResourceScanningServiceRolePolicy

Description : accorde à l' AWS Well-Architected agent un accès en lecture seule aux configurations AWS des ressources, aux paramètres de sécurité et aux données opérationnelles afin de générer des recommandations d'optimisation

AWSWellArchitectedAgentResourceScanningServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 04 août 2026, 17:27 UTC
- Heure modifiée : 24 septembre 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedAgentResourceScanningServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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",
"qlldb:DescribeJournalKinesisStream",
"qlldb:ListJournalKinesisStreamsForLedger",
"qlldb: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:DescribeSenderId",
"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}"
    }
  }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSWellArchitectedDiscoveryServiceRolePolicy

Description : Permet d'accéder WellArchitected à AWS des services et à des ressources liés aux WellArchitected ressources pour le compte des clients.

AWSWellArchitectedDiscoveryServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 26 avril 2023, 18:36 UTC
- Heure modifiée : 26 avril 2023, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedDiscoveryServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"  
    ]  
}  
]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSWellArchitectedOrganizationsServiceRolePolicy

Description : Permet Well-Architected d'accéder aux organisations en votre nom.

AWSWellArchitectedOrganizationsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 23 juin 2022, 17:15 UTC
- Heure modifiée : 25 juillet 2022, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSWickrFullAccess

Description : Cette politique accorde des autorisations administratives complètes au service Wickr, y compris les fonctions administratives de Wickr dans le cadre du. Console de gestion AWS

AWSWickrFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSWickrFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 novembre 2022, 20:36 UTC
- Heure modifiée : 27 novembre 2022, 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWickrFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSXrayCrossAccountSharingConfiguration

Description : fournit des fonctionnalités permettant de gérer les liens du gestionnaire d'accès à l'observabilité et d'établir le partage des traces X-Ray

AWSXrayCrossAccountSharingConfiguration est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSXrayCrossAccountSharingConfiguration à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 novembre 2022, 13:46 UTC
- Heure modifiée : 27 novembre 2022, 13:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayCrossAccountSharingConfiguration`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSXRayDaemonWriteAccess

Description : autorisez le AWS X-Ray démon à transmettre les données brutes des segments de trace à l'API du service et à récupérer les données d'échantillonnage (règles, cibles, etc.) à utiliser par le X-Ray SDK.

AWSXRayDaemonWriteAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `AWSXRayDaemonWriteAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 août 2018, 23:00 UTC
- Heure modifiée : 13 février 2024, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXRayDaemonWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSXrayFullAccess

Description : politique de gestion de l'accès AWS X-Ray complet

AWSXrayFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSXrayFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2016, 18:30 UTC
- Heure modifiée : 11 avril 2024, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
```



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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSXrayReadOnlyAccess

Description : politique gérée en AWS X-Ray lecture seule

AWSXrayReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSXrayReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2016, 18:27 UTC
- Heure modifiée : 14 février 2024, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSXrayWriteOnlyAccess

Description : politique gérée en AWS X-Ray écriture seule

AWSXrayWriteOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer AWSXrayWriteOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2016, 18:19 UTC
- Heure modifiée : 28 août 2018, 23:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "xray:PutTraceSegments",
    "xray:PutTelemetryRecords",
    "xray:GetSamplingRules",
    "xray:GetSamplingTargets",
    "xray:GetSamplingStatisticSummaries"
  ],
  "Resource" : [
    "*"
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSZonalAutoshiftPracticeRunSLRPolicy

Description : Fournit un accès administratif pour les entraînements par quarts de zone ARC, ainsi qu'un accès aux états des CloudWatch alarmes pour surveiller les essais.

AWSZonalAutoshiftPracticeRunSLRPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 29 novembre 2023, 17:34 UTC

- Heure modifiée : 30 juin 2025, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

AWSZoneGroupAccessManagementServiceRolePolicy

Description : fournit un accès en lecture seule aux API nécessaires pour prendre en charge la gestion de l'accès aux groupes de zones pour les organisations.

AWSZoneGroupAccessManagementServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 01 juillet 2025, 19:07 UTC
- Heure modifiée : 01 juillet 2025, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZoneGroupAccessManagementServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

BatchServiceRolePolicy

Description : donne accès au service AWS Batch pour gérer les ressources requises, y compris les ressources Amazon EC2 et Amazon ECS.

BatchServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 10 mars 2021, 06:55 UTC
- Heure modifiée : 05 août 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
    ]
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

BedrockAgentCoreFullAccess

Description : Fournit un accès complet à Bedrock AgentCore ainsi qu'un accès limité aux services connexes

BedrockAgentCoreFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer BedrockAgentCoreFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 16 juillet 2025, 13:37 UTC
- Heure modifiée : 03 septembre 2026, 22:07 UTC
- ARN: `arn:aws:iam::aws:policy/BedrockAgentCoreFullAccess`

Version de la politique

Version de la politique : v21 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

BedrockAgentCoreNetworkServiceRolePolicy

Description : Permet d'accéder aux autres ressources de AWS service nécessaires pour exécuter Amazon Bedrock AgentCore en mode VPC

BedrockAgentCoreNetworkServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 19 septembre 2025, 22:04 UTC
- Heure modifiée : 19 septembre 2025, 22:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/BedrockAgentCoreNetworkServiceRolePolicy

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
}

```

```
]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

BedrockAgentCoreRuntimeIdentityServiceRolePolicy

Description : Permet d'accéder aux ressources de gestion des identités et des jetons nécessaires à l'authentification et à l'autorisation d'Amazon Bedrock AgentCore Runtime.

BedrockAgentCoreRuntimeIdentityServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 11 octobre 2025, 01:04 UTC
- Heure modifiée : 11 octobre 2025, 01:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BedrockAgentCoreRuntimeIdentityServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
  }
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

BedrockAgentCoreRuntimeInstancesInstanceRolePolicy

Description : Politique par défaut pour le rôle d'instance des instances gérées par Bedrock AgentCore Runtime Instances.

BedrockAgentCoreRuntimeInstancesInstanceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer BedrockAgentCoreRuntimeInstancesInstanceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 05 août 2026, 13:27 UTC
- Heure modifiée : 05 août 2026, 13:27 UTC
- ARN: `arn:aws:iam::aws:policy/BedrockAgentCoreRuntimeInstancesInstanceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowWritingSystemLogs",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:PutSystemLogEvents"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:capacity-provider/*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

BedrockAgentCoreRuntimeInstancesOperatorRolePolicy

Description : Permet de créer et de gérer les ressources de calcul et les ressources associées pour les instances Bedrock AgentCore Runtime

BedrockAgentCoreRuntimeInstancesOperatorRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer BedrockAgentCoreRuntimeInstancesOperatorRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 août 2026, 11:27 UTC
- Heure modifiée : 06 août 2026, 10:12 UTC
- ARN: `arn:aws:iam::aws:policy/BedrockAgentCoreRuntimeInstancesOperatorRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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.*"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

Facturation

Description : octroie des autorisations pour la gestion de la facturation et des coûts. Cela inclut la visualisation de l'utilisation du compte ainsi que la consultation et la modification des budgets et des modes de paiement.

Billing est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer Billing à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux fonctions
- Heure de création : 10 novembre 2016, 17:33 UTC
- Heure modifiée : 30 juillet 2026, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/Billing`

Version de la politique

Version de la politique : v30 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

BudgetsServiceRolePolicy

Description : permet à Budgets de vérifier l'accès aux vues de facturation partagées au-delà des limites des comptes.

BudgetsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 30 juillet 2025, 21:07 UTC
- Heure modifiée : 30 juillet 2025, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BudgetsServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CertificateManagerServiceRolePolicy

Description : Politique relative aux rôles du service Amazon Certificate Manager

CertificateManagerServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 25 juin 2020, 17:56 UTC
- Heure modifiée : 25 juin 2020, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate"
      ]
    }
  ],
}
```

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ClientVPNServiceConnectionsRolePolicy

Description : Politique permettant au VPN AWS client de gérer les connexions de vos terminaux VPN client.

ClientVPNServiceConnectionsRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 12 août 2020, 19:48 UTC
- Heure modifiée : 12 août 2020, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ClientVPNServiceRolePolicy

Description : Politique permettant au VPN AWS client de gérer vos points de terminaison VPN client.

ClientVPNServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 10 décembre 2018, 21:20 UTC
- Heure modifiée : 12 août 2020, 19:39 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudFormationStackSetsOrgAdminServiceRolePolicy

Description : Rôle de service pour CloudFormation StackSets (compte principal de l'organisation)

CloudFormationStackSetsOrgAdminServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 10 décembre 2019, 00:20 UTC
- Heure modifiée : 10 décembre 2019, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudFormationStackSetsOrgMemberServiceRolePolicy

Description : Rôle de service pour CloudFormation StackSets (compte de membre de l'organisation)

CloudFormationStackSetsOrgMemberServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 09 décembre 2019, 23:52 UTC
- Heure modifiée : 22 juillet 2026, 20:12 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudFrontFullAccess

Description : fournit un accès complet à la CloudFront console et la possibilité de répertorier les compartiments Amazon S3 via le Console de gestion AWS.

CloudFrontFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `CloudFrontFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:39 UTC
- Heure modifiée : 30 juillet 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontFullAccess`

Version de la politique

Version de la politique : v15 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfflistbuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "cfffullaccess",
      "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:*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudFrontReadOnlyAccess

Description : Permet d'accéder aux informations de configuration de la CloudFront distribution et de répertorier les distributions via le Console de gestion AWS.

CloudFrontReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudFrontReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:39 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudHSMServiceRolePolicy

Description : Permet d'accéder aux AWS ressources utilisées ou gérées par CloudHSM

CloudHSMServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 06 novembre 2017, 19:12 UTC
- Heure modifiée : 06 novembre 2017, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudSearchFullAccess

Description : fournit un accès complet au service CloudSearch de configuration Amazon.

CloudSearchFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudSearchFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:39 UTC
- Heure modifiée : 06 février 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudSearchReadOnlyAccess

Description : fournit un accès en lecture seule au service CloudSearch de configuration Amazon.

CloudSearchReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudSearchReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:39 UTC
- Heure modifiée : 06 février 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudTrailEventContext

Description : Ce rôle lié à un service permet CloudTrail d'obtenir et d'ajouter des balises de ressource aux CloudTrail événements du propriétaire de la ressource.

CloudTrailEventContext est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 15 mai 2025, 13:52 UTC
- Heure modifiée : 15 mai 2025, 13:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailEventContext`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudTrailServiceRolePolicy

Description : Politique d'autorisation pour CloudTrail ServiceLinkedRole

CloudTrailServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 24 octobre 2018, 21:21 UTC
- Heure modifiée : 27 novembre 2023, 01:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  }
}

```

```
}  
]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatch-CrossAccountAccess

Description : Permet CloudWatch d'assumer CloudWatch-CrossAccountSharing des rôles dans des comptes distants pour le compte courant afin d'afficher les données entre comptes et régions

CloudWatch-CrossAccountAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 23 juillet 2019, 09:59 UTC
- Heure modifiée : 23 juillet 2019, 09:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
      ],
      "Effect" : "Allow"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchActionsEC2Access

Description : fournit un accès en lecture seule aux CloudWatch alarmes et aux mesures ainsi qu'aux métadonnées EC2. Permet d'accéder aux instances EC2 pour arrêter, arrêter et redémarrer.

CloudWatchActionsEC2Access est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchActionsEC2Access à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 juillet 2015, 00:00 UTC
- Heure modifiée : 07 juillet 2015, 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchActionsEC2Access`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchAgentAdminPolicy

Description : Autorisations complètes requises pour l'utiliser AmazonCloudWatchAgent.

CloudWatchAgentAdminPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `CloudWatchAgentAdminPolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 mars 2018, 00:52 UTC
- Heure modifiée : 05 février 2024, 20:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchAgentServerPolicy

Description : Autorisations requises pour une utilisation AmazonCloudWatchAgent sur les serveurs

CloudWatchAgentServerPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchAgentServerPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 mars 2018, 01:06 UTC
- Heure modifiée : 06 février 2024, 16:37 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
    }
  ]
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchAPIKeyAccess

Description : accorde des autorisations d'appel à CloudWatch l'aide de l'authentification par clé API.

CloudWatchAPIKeyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchAPIKeyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 mai 2026, 08:57 UTC
- Heure modifiée : 04 juin 2026, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAPIKeyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchApplicationInsightsFullAccess

Description : fournit un accès complet à CloudWatch Application Insights et aux dépendances requises.

CloudWatchApplicationInsightsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchApplicationInsightsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 novembre 2020, 18:44 UTC
- Heure modifiée : 25 janvier 2022, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchApplicationInsightsReadOnlyAccess

Description : fournit un accès en lecture seule à CloudWatch Application Insights.

CloudWatchApplicationInsightsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchApplicationInsightsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 novembre 2020, 18:48 UTC
- Heure modifiée : 24 novembre 2020, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
        "applicationinsights:Describe*",
        "applicationinsights:List*"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudwatchApplicationInsightsServiceLinkedRolePolicy

Description : Politique relative aux rôles liés au service Cloudwatch Application Insights

CloudwatchApplicationInsightsServiceLinkedRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 01 décembre 2018, 16:22 UTC
- Heure modifiée : 25 juillet 2024, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy`

Version de la politique

Version de la politique : v25 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
      "*"
    ]
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchApplicationSignalsFullAccess

Description : Fournissez un accès complet au service CloudWatch Application Signals et un accès limité aux dépendances nécessaires à l'utilisation et à l'exploitation de ce service.

CloudWatchApplicationSignalsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchApplicationSignalsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 juin 2024, 22:50 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsFullAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchApplicationSignalsReadOnlyAccess

Description : fournit un accès en lecture seule au service CloudWatch Application Signals et un accès limité aux dépendances nécessaires à l'utilisation de ce service

CloudWatchApplicationSignalsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `CloudWatchApplicationSignalsReadOnlyAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 juin 2024, 22:48 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsReadOnlyAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:BatchGetRunMetricDefinitions",
      "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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchApplicationSignalsServiceRolePolicy

Description : La politique autorise CloudWatch Application Signals à collecter des données de surveillance et de balisage auprès d'autres AWS services concernés.

CloudWatchApplicationSignalsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 09 novembre 2023, 18:09 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy`

Version de la politique

Version de la politique : v11 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchAutomaticDashboardsAccess

Description : donne accès aux CloudWatch non-API utilisées pour afficher les tableaux de bord CloudWatch automatiques, y compris le contenu d'objets tels que les fonctions Lambda

CloudWatchAutomaticDashboardsAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchAutomaticDashboardsAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 juillet 2019, 10:01 UTC
- Heure modifiée : 07 août 2026, 10:42 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchCrossAccountSharingConfiguration

Description : fournit des fonctionnalités permettant de gérer les liens du gestionnaire d'accès à l'observabilité et d'établir le partage des ressources CloudWatch

CloudWatchCrossAccountSharingConfiguration est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchCrossAccountSharingConfiguration à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 novembre 2022, 14:01 UTC
- Heure modifiée : 27 novembre 2022, 14:01 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchCrossAccountSharingConfiguration`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchEventsBuiltInTargetExecutionAccess

Description : permet aux cibles intégrées dans Amazon CloudWatch Events d'effectuer des actions EC2 en votre nom.

CloudWatchEventsBuiltInTargetExecutionAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `CloudWatchEventsBuiltInTargetExecutionAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 14 janvier 2016, 18:35 UTC
- Heure modifiée : 14 janvier 2016, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchEventsFullAccess

Description : fournit un accès complet à Amazon CloudWatch Events.

CloudWatchEventsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchEventsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 janvier 2016, 18:37 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsFullAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchEventsInvocationAccess

Description : permet à Amazon CloudWatch Events de relayer les événements vers les flux de AWS Kinesis Streams de votre compte.

CloudWatchEventsInvocationAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchEventsInvocationAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 14 janvier 2016, 18:36 UTC
- Heure modifiée : 14 janvier 2016, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsInvocationAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord"
      ]
    }
  ]
}
```

```
    ],  
    "Resource" : "*"br/>  }  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchEventsReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon CloudWatch Events.

CloudWatchEventsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchEventsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 14 janvier 2016, 18:27 UTC
- Heure modifiée : 01 décembre 2022, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchEventsServiceRolePolicy

Description : Permet d' AWS CloudWatch exécuter des actions en votre nom configurées par le biais d'alarmes et d'événements.

CloudWatchEventsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 17 novembre 2017, 00:42 UTC
- Heure modifiée : 17 novembre 2017, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchFullAccess

Description : fournit un accès complet à CloudWatch.

CloudWatchFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 27 novembre 2022, 13:23 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    }
  ]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchFullAccessV2

Description : fournit un accès complet à CloudWatch.

CloudWatchFullAccessV2 est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchFullAccessV2 à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 août 2023, 11:32 UTC
- Heure modifiée : 22 septembre 2026, 16:57 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchFullAccessV2

Version de la politique

Version de la politique : v17 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchInternetMonitorFullAccess

Description : fournit un accès complet aux actions permettant d'utiliser Amazon CloudWatch Internet Monitor. Permet également d'accéder à d'autres services, tels qu'Amazon CloudWatch, Amazon EC2 CloudFront WorkSpaces, Amazon et Elastic Load Balancing, nécessaires à l'utilisation du service Internet Monitor pour surveiller et stocker des informations sur le trafic des applications.

CloudWatchInternetMonitorFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchInternetMonitorFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 octobre 2024, 21:02 UTC
- Heure modifiée : 22 octobre 2024, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchInternetMonitorFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchInternetMonitorReadOnlyAccess

Description : fournit un accès en lecture seule aux actions permettant d'utiliser Amazon CloudWatch Internet Monitor. Permet également d'accéder à d'autres services d'Amazon CloudWatch, notamment des politiques permettant de récupérer des informations sur CloudWatch les métriques et de gérer les requêtes de journal, nécessaires à l'utilisation du service Internet Monitor pour surveiller et stocker des informations sur le trafic des applications.

CloudWatchInternetMonitorReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchInternetMonitorReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 novembre 2024, 23:11 UTC
- Heure modifiée : 12 novembre 2024, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchInternetMonitorReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchInternetMonitorServiceRolePolicy

Description : permet à Internet Monitor d'accéder à EC2, aux espaces de travail et aux CloudFront ressources, ainsi qu'à d'autres services requis en votre nom.

CloudWatchInternetMonitorServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 27 novembre 2022, 17:46 UTC
- Heure modifiée : 20 juillet 2023, 04:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchLambdaApplicationSignalsExecutionRolePolicy

Description : fournit un accès en écriture à un groupe X-Ray de journaux des signaux d' CloudWatch application.

CloudWatchLambdaApplicationSignalsExecutionRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchLambdaApplicationSignalsExecutionRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 16 octobre 2024, 19:09 UTC
- Heure modifiée : 16 octobre 2024, 19:09 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLambdaApplicationSignalsExecutionRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchLambdaInsightsExecutionRolePolicy

Description : Politique requise pour l'extension Lambda Insights

CloudWatchLambdaInsightsExecutionRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `CloudWatchLambdaInsightsExecutionRolePolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 octobre 2020, 19:27 UTC
- Heure modifiée : 07 octobre 2020, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*"
    }
  ]
}
```



```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchLogsAPIKeyAccess

Description : accorde des autorisations pour appeler CloudWatch Logs à l'aide de l'authentification par clé API.

CloudWatchLogsAPIKeyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchLogsAPIKeyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 février 2026, 19:42 UTC
- Heure modifiée : 20 février 2026, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsAPIKeyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "KMSSDescribeAPIs",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "logs.*.amazonaws.com"
        }
      },
      "Resource" : "arn:aws:kms:*:*:key/*"
    }
  ]
}
```

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchLogsCrossAccountSharingConfiguration

Description : fournit des fonctionnalités permettant de gérer les liens d'Observability Access Manager et d'établir le partage des ressources des CloudWatch journaux

CloudWatchLogsCrossAccountSharingConfiguration est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchLogsCrossAccountSharingConfiguration à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 novembre 2022, 13:55 UTC
- Heure modifiée : 27 novembre 2022, 13:55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchLogsFullAccess

Description : fournit un accès complet aux CloudWatch journaux

CloudWatchLogsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchLogsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsFullAccess`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
{
  "Sid" : "CloudWatchLogsFullAccess",
  "Effect" : "Allow",
  "Action" : [
    "logs:*",
    "cloudwatch:GenerateQuery",
    "cloudwatch:GenerateQueryResultsSummary",
    "observabilityadmin:GetS3TableIntegration",
    "observabilityadmin:ListS3TableIntegrations",
    "observabilityadmin:ListTelemetryPipelines"
  ],
  "Resource" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchLogsReadOnlyAccess

Description : fournit un accès en lecture seule aux CloudWatch journaux

CloudWatchLogsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchLogsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchNetworkFlowMonitorAgentPublishPolicy

Description : Vous pouvez utiliser cette politique dans les rôles IAM associés aux ressources d'instance Amazon EC2 et Amazon EKS pour envoyer des rapports de télémétrie (métriques) à un point de terminaison Network Flow Monitor.

CloudWatchNetworkFlowMonitorAgentPublishPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchNetworkFlowMonitorAgentPublishPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2024, 22:51 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchNetworkFlowMonitorAgentPublishPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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



```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "networkflowmonitor:Publish"
    ],
    "Resource" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchNetworkFlowMonitorServiceRolePolicy

Description : Vous ne pouvez pas vous connecter

CloudWatchNetworkFlowMonitorServiceRolePolicy à vos entités IAM. Cette politique est associée à un rôle lié à un service nommé AWSServiceRoleForNetworkFlowMonitor, qui publie les résultats d'agrégation de la télémétrie réseau, collectés par les agents Network Flow Monitor, à CloudWatch. Il permet également au service d'utiliser les AWS organisations pour obtenir des informations sur des scénarios multi-comptes.

CloudWatchNetworkFlowMonitorServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 01 décembre 2024, 22:36 UTC

- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkFlowMonitorServiceRolePolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
]
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy

Description : Vous ne pouvez pas vous connecter CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy à vos entités IAM. Cette politique est associée à un rôle lié à un service nommé AWSServiceRoleForNetworkFlowMonitor _Topology, qui génère des instantanés de topologie des ressources utilisées par Network Flow Monitor sur votre compte.

CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 01 décembre 2024, 22:51 UTC
- Heure modifiée : 01 septembre 2026, 01:47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchNetworkMonitorServiceRolePolicy

Description : Permet à CloudWatch Network Monitor d'accéder aux ressources EC2 et VPC et de les gérer, de publier des données CloudWatch et d'accéder à d'autres services requis en votre nom.

CloudWatchNetworkMonitorServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 21 décembre 2023, 18:53 UTC
- Heure modifiée : 25 août 2026, 13:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
}

```



```
]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchOmniAWSIntegrationPolicy

Description : fournit les autorisations requises par CloudWatch Omni pour découvrir et lire la topologie AWS des ressources

CloudWatchOmniAWSIntegrationPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchOmniAWSIntegrationPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 septembre 2026, 04:07 UTC
- Heure modifiée : 22 septembre 2026, 04:07 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOmniAWSIntegrationPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchOmniDomainAccessPolicy

Description : fournit les autorisations nécessaires pour gérer l'accès CloudWatch au domaine Omni.

CloudWatchOmniDomainAccessPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchOmniDomainAccessPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 septembre 2026, 01:47 UTC
- Heure modifiée : 22 septembre 2026, 01:47 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchOmniDomainAccessPolicy

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchOmniModelInferencePolicy

Description : Politique gérée permettant aux clients de se connecter à CloudWatch Omni afin que CloudWatch les fonctionnalités d'Omni puissent effectuer des appels d'inférence du modèle Bedrock, par exemple dans Agent Playground ou Evaluations

CloudWatchOmniModelInferencePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchOmniModelInferencePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 septembre 2026, 01:47 UTC
- Heure modifiée : 22 septembre 2026, 01:47 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOmniModelInferencePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchOmniSpaceAccessPolicy

Description : Permet de gérer les espaces CloudWatch Omni, d'afficher les applications, la télémétrie et d'autres fonctionnalités d'observabilité et de surveillance via le nouveau produit Omni CloudWatch

CloudWatchOmniSpaceAccessPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchOmniSpaceAccessPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 septembre 2026, 01:47 UTC
- Heure modifiée : 22 septembre 2026, 01:47 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOmniSpaceAccessPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchOpenSearchDashboardAccess

Description : Cette politique permet aux utilisateurs d'accéder aux OpenSearch tableaux de bord sur la console CloudWatch Logs.

CloudWatchOpenSearchDashboardAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchOpenSearchDashboardAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2024, 21:06 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOpenSearchDashboardAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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_*"
}

```



```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchOpenSearchDashboardsFullAccess

Description : Cette politique permet aux utilisateurs d'accéder à des tableaux de bord OpenSearch pour créer, mettre à jour, supprimer ou afficher des tableaux de bord sur la console CloudWatch Logs.

CloudWatchOpenSearchDashboardsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchOpenSearchDashboardsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2024, 21:06 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOpenSearchDashboardsFullAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchReadOnlyAccess

Description : fournit un accès en lecture seule à CloudWatch.

CloudWatchReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 22 septembre 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess`

Version de la politique

Version de la politique : v25 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ]
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchSyntheticsFullAccess

Description : fournit un accès complet à CloudWatch Synthetics.

CloudWatchSyntheticsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchSyntheticsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 novembre 2019, 17:39 UTC
- Heure modifiée : 31 mars 2026, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess`

Version de la politique

Version de la politique : v14 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      ]
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CloudWatchSyntheticsReadOnlyAccess

Description : fournit un accès en lecture seule à CloudWatch Synthetics.

CloudWatchSyntheticsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CloudWatchSyntheticsReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 novembre 2019, 17:45 UTC
- Heure modifiée : 06 mars 2020, 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ComprehendDataAccessRolePolicy

Description : Stratégie pour le rôle de service AWS Comprehend qui permet d'accéder aux ressources S3 pour l'accès aux données

ComprehendDataAccessRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ComprehendDataAccessRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 06 mars 2019, 22:28 UTC
- Heure modifiée : 06 mars 2019, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::*Comprehend*",
      "arn:aws:s3:::*comprehend*"
    ]
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ComprehendFullAccess

Description : fournit un accès complet à Amazon Comprehend.

ComprehendFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `ComprehendFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2017, 18:08 UTC
- Heure modifiée : 05 décembre 2017, 01:36 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehend:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ComprehendMedicalFullAccess

Description : fournit un accès complet à Amazon Comprehend Medical

ComprehendMedicalFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ComprehendMedicalFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 novembre 2018, 17:55 UTC
- Heure modifiée : 27 novembre 2018, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendMedicalFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
{
  "Action" : [
    "comprehendmedical:*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ComprehendReadOnly

Description : fournit un accès en lecture seule à Amazon Comprehend.

ComprehendReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ComprehendReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2017, 18:10 UTC
- Heure modifiée : 26 avril 2022, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendReadOnly`

Version de la politique

Version de la politique : v11 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ComputeOptimizerAutomationServiceRolePolicy

Description : La politique ComputeOptimizerAutomationServiceRolePolicy gérée est associée à un rôle lié à un service qui permet à Compute Optimizer d'effectuer des actions en votre nom

ComputeOptimizerAutomationServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 15 novembre 2025, 01:19 UTC
- Heure modifiée : 15 novembre 2025, 01:19 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerAutomationServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            ]
        }
    }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ComputeOptimizerReadOnlyAccess

Description : fournit un accès en lecture seule à ComputeOptimizer.

ComputeOptimizerReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ComputeOptimizerReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 07 mars 2020, 00:11 UTC
- Heure modifiée : 20 novembre 2024, 21:08 UTC
- ARN: `arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ComputeOptimizerServiceRolePolicy

Description : Permet d' ComputeOptimizer appeler les AWS services et de recueillir des informations sur la charge de travail en votre nom.

ComputeOptimizerServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 03 décembre 2019, 08:45 UTC
- Heure modifiée : 27 mai 2026, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ConfigConformsServiceRolePolicy

Description : Politique requise pour qu'AWSConfig crée des packs de conformité

ConfigConformsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 25 juillet 2019, 21:38 UTC
- Heure modifiée : 12 janvier 2023, 04:17 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ConsoleFullAccessFromVercel

Description : À utiliser avec les comptes créés via l'intégration de Vercel Marketplace avec AWS. Permet de gérer toutes les ressources des services intégrés à Vercel Marketplace.

ConsoleFullAccessFromVercel est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ConsoleFullAccessFromVercel à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 décembre 2025, 16:49 UTC
- Heure modifiée : 09 avril 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/ConsoleFullAccessFromVercel`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ConsoleViewOnlyAccessFromVercel

Description : À utiliser avec les comptes créés via l'intégration de Vercel Marketplace avec AWS. Permet d'accéder à toutes les ressources relatives aux services intégrés à Vercel Marketplace.

ConsoleViewOnlyAccessFromVercel est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ConsoleViewOnlyAccessFromVercel à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 décembre 2025, 16:49 UTC
- Heure modifiée : 09 avril 2026, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/ConsoleViewOnlyAccessFromVercel`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CostOptimizationHubAdminAccess

Description : Cette politique gérée fournit un accès administrateur à Cost Optimization Hub.

CostOptimizationHubAdminAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CostOptimizationHubAdminAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 décembre 2023, 00:03 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            ]
        }
    }
}

```



```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CostOptimizationHubReadOnlyAccess

Description : Cette politique gérée fournit un accès en lecture seule à Cost Optimization Hub.

CostOptimizationHubReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer CostOptimizationHubReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 décembre 2023, 18:04 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubReadOnlyAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CostOptimizationHubServiceRolePolicy

Description : permet à Cost Optimization Hub de récupérer des informations sur l'organisation et de collecter des données et des métadonnées liées à l'optimisation.

CostOptimizationHubServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 26 novembre 2023, 08:03 UTC
- Heure modifiée : 17 juillet 2025, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "*"
    ]
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

CustomerProfilesServiceLinkedRolePolicy

Description : permet aux profils clients Amazon Connect d'accéder aux AWS services et aux ressources en votre nom.

CustomerProfilesServiceLinkedRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 07 mars 2023, 22:56 UTC
- Heure modifiée : 05 mars 2026, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CustomerProfilesServiceLinkedRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

DatabaseAdministrator

Description : accorde des autorisations d'accès complètes aux AWS services et aux actions requises pour configurer et configurer les services AWS de base de données.

DatabaseAdministrator est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer DatabaseAdministrator à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux fonctions
- Heure de création : 10 novembre 2016, 17:25 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DatabaseAdministrator`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ]
}
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

DataScientist

Description : accorde des autorisations aux services d'analyse de AWS données.

DataScientist est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer DataScientist à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux fonctions
- Heure de création : 10 novembre 2016, 17:28 UTC
- Heure modifiée : 02 septembre 2026, 23:37 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DataScientist`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ]
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

DAXServiceRolePolicy

Description : Cette politique permet à DAX de créer et de gérer une interface réseau, un groupe de sécurité, un sous-réseau et un VPC pour le compte du client

DAXServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 05 mars 2018, 17:51 UTC
- Heure modifiée : 05 mars 2018, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

DBModDiscoveryAndAssessment

Description : autorisations de découverte et d'évaluation pour le connecteur de base de données utilisé dans le cadre de la modernisation de la base de données

DBModDiscoveryAndAssessment est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer DBModDiscoveryAndAssessment à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 mars 2026, 20:27 UTC
- Heure modifiée : 25 mars 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/DBModDiscoveryAndAssessment`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

DBModProvisioningAndMigration

Description : autorisations de provisionnement des ressources et de migration des données pour le connecteur de base de données utilisé dans le cadre de la modernisation de la base de données

DBModProvisioningAndMigration est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer DBModProvisioningAndMigration à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 mars 2026, 20:42 UTC

- Heure modifiée : 25 mars 2026, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/DBModProvisioningAndMigration`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
    }
}
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

DBModVirtualSource

Description : fournit des autorisations pour le connecteur de base de données utilisé par ATxHelix lors du flux de modernisation de base de données hors ligne (DMS-free)

DBModVirtualSource est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer DBModVirtualSource à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 juillet 2026, 23:12 UTC
- Heure modifiée : 06 juillet 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/DBModVirtualSource`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"  
    }  
  }  
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

DeclarativePoliciesEC2Report

Description : donne accès aux API en lecture seule nécessaires à l'exécution du rapport sur l'état du compte EC2 Declarative Policies.

DeclarativePoliciesEC2Report est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 30 novembre 2024, 13:21 UTC
- Heure modifiée : 03 juillet 2026, 10:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DeclarativePoliciesEC2Report`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

Description : autorisations requises pour prendre en charge Amazon CloudWatch Contributor Insights pour Amazon DynamoDB.

DynamoDBCloudWatchContributorInsightsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 15 novembre 2019, 21:13 UTC
- Heure modifiée : 15 novembre 2019, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

DynamoDBGlobalTableSettingsManagementServiceRolePolicy

Description : autorisations requises par DynamoDB pour gérer les paramètres de réplication de tables globales

DynamoDBGlobalTableSettingsManagementServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 15 octobre 2025, 17:34 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBGlobalTableSettingsManagementServiceRolePolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    ]
  }
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

DynamoDBKinesisReplicationServiceRolePolicy

Description : Fournir un accès AWS DynamoDB à KinesisDataStreams

DynamoDBKinesisReplicationServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 12 novembre 2020, 00:43 UTC
- Heure modifiée : 12 novembre 2020, 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

DynamoDBReplicationServiceRolePolicy

Description : autorisations requises par DynamoDB pour la réplication de données entre régions

DynamoDBReplicationServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 09 novembre 2017, 23:55 UTC
- Heure modifiée : 08 janvier 2024, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            ]
        }
    }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

EC2ApplicationStatusChecksServiceRolePolicy

Description : Permet à EC2 de découvrir et de gérer les ressources liées aux vérifications de l'état des applications EC2

EC2ApplicationStatusChecksServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 27 avril 2026, 23:42 UTC
- Heure modifiée : 15 juillet 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2ApplicationStatusChecksServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

EC2FastLaunchFullAccess

Description : Cette politique accorde un accès complet aux actions EC2 Fast Launch

EC2FastLaunchFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer EC2FastLaunchFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 mai 2024, 22:45 UTC
- Heure modifiée : 04 août 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/EC2FastLaunchFullAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
          ]
        }
      }
    }
  ]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

EC2FastLaunchServiceRolePolicy

Description : La politique autorise ec2fastlaunch à préparer et à gérer les instantanés préprovisionnés sur le compte du client et à publier les mesures associées.

EC2FastLaunchServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 10 janvier 2022, 13:08 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

EC2FleetTimeShiftableServiceRolePolicy

Description : Politique autorisant EC2 Fleet à lancer des instances dans le futur.

EC2FleetTimeShiftableServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 23 décembre 2019, 19:47 UTC
- Heure modifiée : 23 décembre 2019, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  }
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

Ec2ImageBuilderCrossAccountDistributionAccess

Description : autorisations requises par EC2 Image Builder pour effectuer une distribution entre comptes.

Ec2ImageBuilderCrossAccountDistributionAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer Ec2ImageBuilderCrossAccountDistributionAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 septembre 2020, 19:22 UTC
- Heure modifiée : 30 septembre 2020, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/Ec2ImageBuilderCrossAccountDistributionAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

EC2ImageBuilderExecutionPolicy

Description : accorde des autorisations qui permettent à EC2 Image Builder d'appeler AWS les services en votre nom

EC2ImageBuilderExecutionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer EC2ImageBuilderExecutionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 juin 2026, 17:12 UTC

- Heure modifiée : 08 juillet 2026, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/EC2ImageBuilderExecutionPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

EC2ImageBuilderLifecycleExecutionPolicy

Description : La EC2ImageBuilderLifecycleExecutionPolicy politique autorise Image Builder à effectuer des actions telles que rendre obsolètes ou supprimer les ressources d'image Image Builder et leurs ressources sous-jacentes (AMI, instantanés) afin de prendre en charge les règles automatisées pour les tâches de gestion du cycle de vie des images.

EC2ImageBuilderLifecycleExecutionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `EC2ImageBuilderLifecycleExecutionPolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 16 novembre 2023, 23:23 UTC
- Heure modifiée : 16 novembre 2023, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

EC2InstanceConnect

Description : permet aux clients d'appeler EC2 Instance Connect pour publier des clés éphémères sur leurs instances EC2 et de se connecter via SSH ou l'interface de ligne de commande EC2 Instance Connect.

EC2InstanceConnect est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer EC2InstanceConnect à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 juin 2019, 18:53 UTC
- Heure modifiée : 27 juin 2019, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceConnect`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceConnect",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2-instance-connect:SendSSHPublicKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

Ec2InstanceConnectEndpoint

Description : Politique relative aux terminaux EC2 Instance Connect pour gérer les terminaux EC2 Instance Connect créés par le client

Ec2InstanceConnectEndpoint est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 24 janvier 2023, 20:19 UTC
- Heure modifiée : 31 juillet 2025, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
        ]
      }
    }
  }
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

EC2InstanceProfileForImageBuilder

Description : profil d'instance EC2 pour le service Image Builder.

EC2InstanceProfileForImageBuilder est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer EC2InstanceProfileForImageBuilder à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 décembre 2019, 19:08 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

EC2InstanceProfileForImageBuilderECRContainerBuilds

Description : profil d'instance EC2 pour créer des images de conteneurs avec EC2 Image Builder. Cette politique accorde à l'utilisateur de larges autorisations pour télécharger des images ECR.

EC2InstanceProfileForImageBuilderECRContainerBuilds est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer EC2InstanceProfileForImageBuilderECRContainerBuilds à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 décembre 2020, 19:48 UTC
- Heure modifiée : 11 décembre 2020, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ECRReplicationServiceRolePolicy

Description : Permet d'accéder à ECR Services AWS Replication et aux ressources utilisées ou gérées par ECR Replication

ECRReplicationServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 04 décembre 2020, 22:11 UTC
- Heure modifiée : 04 décembre 2020, 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ECRTemplateServiceRolePolicy

Description : Permet d'effectuer des actions lors de l'utilisation de modèles de création de référentiels AWS ECR

ECRTemplateServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 19 juin 2024, 23:11 UTC
- Heure modifiée : 19 juin 2024, 23:11 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRTemplateServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ElastiCacheServiceRolePolicy

Description : Cette politique permet ElastiCache de gérer les AWS ressources en votre nom si nécessaire à la gestion de votre cache

ElastiCacheServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 07 décembre 2017, 17:50 UTC
- Heure modifiée : 28 novembre 2023, 03:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/AmazonElasticCacheManaged" : "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/*"
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ElasticLoadBalancingFullAccess

Description : fournit un accès complet à Amazon ElasticLoadBalancing et un accès limité aux autres services nécessaires à la fourniture de ElasticLoadBalancing fonctionnalités.

ElasticLoadBalancingFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ElasticLoadBalancingFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 septembre 2018, 20:42 UTC

- Heure modifiée : 23 février 2026, 18:57 UTC
- ARN: arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ElasticLoadBalancingReadOnly

Description : fournit un accès en lecture seule à Amazon ElasticLoadBalancing et aux services dépendants

ElasticLoadBalancingReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ElasticLoadBalancingReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 septembre 2018, 20:17 UTC
- Heure modifiée : 26 novembre 2023, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ElementalActivationsDownloadSoftwareAccess

Description : Accès à la visualisation des actifs achetés et au téléchargement des logiciels associés et des fichiers kickstart

ElementalActivationsDownloadSoftwareAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `ElementalActivationsDownloadSoftwareAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 08 septembre 2020, 17:26 UTC
- Heure modifiée : 08 septembre 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ElementalActivationsFullAccess

Description : Accès complet pour consulter et agir sur les actifs achetés par Elemental Appliances et Software

ElementalActivationsFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ElementalActivationsFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 juin 2020, 21:00 UTC
- Heure modifiée : 04 juin 2020, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
"Action" : [
  "elemental-activations:*"
],
"Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ElementalActivationsGenerateLicenses

Description : Accès à la visualisation des actifs achetés et à la génération de licences logicielles pour les activations en attente

ElementalActivationsGenerateLicenses est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ElementalActivationsGenerateLicenses à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 août 2020, 18:28 UTC
- Heure modifiée : 28 août 2020, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ElementalActivationsReadOnlyAccess

Description : Read-only accès à la liste détaillée des actifs achetés associés au nom Compte AWS de l'utilisateur

ElementalActivationsReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `ElementalActivationsReadOnlyAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 août 2020, 16:51 UTC
- Heure modifiée : 28 août 2020, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ElementalAppliancesSoftwareFullAccess

Description : Accès complet pour consulter les devis et les commandes d'appareils et de logiciels Elemental et prendre des mesures en conséquence

ElementalAppliancesSoftwareFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ElementalAppliancesSoftwareFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 31 juillet 2019, 16:28 UTC
- Heure modifiée : 05 février 2021, 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
        "elemental-appliances-software:*",
        "elemental-activations:CompleteAccountRegistration"
    ],
    "Resource" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ElementalAppliancesSoftwareReadOnlyAccess

Description : Read-only accès pour consulter les devis et les commandes d'appareils et de logiciels Elemental

ElementalAppliancesSoftwareReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ElementalAppliancesSoftwareReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 01 avril 2020, 22:31 UTC
- Heure modifiée : 01 avril 2020, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ElementalSupportCenterFullAccess

Description : Accès complet pour consulter les dossiers de support des appliances et des logiciels Elemental et prendre des mesures à leur sujet, ainsi que le contenu du support produit

ElementalSupportCenterFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ElementalSupportCenterFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 novembre 2020, 18:08 UTC
- Heure modifiée : 05 février 2021, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-support-cases:*",
        "elemental-support-content:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

EMRDescribeClusterPolicyForEMRWAL

Description : Cette politique accorde des autorisations en lecture seule qui permettent au service WAL pour Amazon EMR de rechercher et de renvoyer l'état d'un cluster

EMRDescribeClusterPolicyForEMRWAL est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 15 juin 2023, 23:30 UTC
- Heure modifiée : 15 juin 2023, 23:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

EndUserMessagingServiceRolePolicy

Description : Permet EndUserMessaging de publier des CloudWatch statistiques en votre nom

EndUserMessagingServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 29 septembre 2026, 19:37 UTC
- Heure modifiée : 29 septembre 2026, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EndUserMessagingServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

FinOpsAgentAgentPolicy

Description : fournit les autorisations requises par l' AWS FinOps agent pour effectuer une analyse des coûts et identifier les opportunités de réduction des coûts sur les AWS ressources des clients.

FinOpsAgentAgentPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer FinOpsAgentAgentPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 juin 2026, 19:57 UTC
- Heure modifiée : 02 octobre 2026, 18:27 UTC

- ARN: `arn:aws:iam::aws:policy/FinOpsAgentAgentPolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

FinOpsAgentOperatorPolicy

Description : permet d'utiliser l'application Web AWS FinOps Agent pour un agent.

FinOpsAgentOperatorPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer FinOpsAgentOperatorPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 juin 2026, 19:57 UTC
- Heure modifiée : 03 juin 2026, 19:57 UTC

- ARN: `arn:aws:iam::aws:policy/FinOpsAgentOperatorPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

FMSServiceRolePolicy

Description : Politique d'accès permettant au rôle lié au service FM d'effectuer des FM-related actions sur les FM-managed ressources du compte d'une AWS organisation cliente.

FMSServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 28 mars 2018, 23:01 UTC
- Heure modifiée : 06 avril 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy`

Version de la politique

Version de la politique : v37 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*:*:vpccorin/*"
},
{
    "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" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

FSxDeleteServiceLinkedRoleAccess

Description : Permet à Amazon FSx de supprimer ses rôles liés aux services pour accéder à Amazon S3

FSxDeleteServiceLinkedRoleAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 28 novembre 2018, 10:40 UTC
- Heure modifiée : 28 novembre 2018, 10:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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_*"
}
]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

GameLiftContainerFleetPolicy

Description : accorde les autorisations requises pour les actions de calcul dans une flotte de GameLift conteneurs Amazon, y compris l'accès à des dépendances telles qu'Amazon S3.

GameLiftContainerFleetPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer GameLiftContainerFleetPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 12 novembre 2024, 19:28 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: arn:aws:iam::aws:policy/GameLiftContainerFleetPolicy

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

GameLiftGameServerGroupPolicy

Description : Politique permettant à Gamelift de gérer les GameServerGroups ressources des clients

GameLiftGameServerGroupPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer GameLiftGameServerGroupPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 avril 2020, 23:12 UTC
- Heure modifiée : 13 mai 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

GitLabDuoWithAmazonQPermissionsPolicy

Description : Cette politique gérée autorise la connexion à Amazon Q et l'utilisation des fonctionnalités de l'intégration GitLab Duo avec Amazon Q.

GitLabDuoWithAmazonQPermissionsPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `GitLabDuoWithAmazonQPermissionsPolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 16 avril 2025, 16:37 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/GitLabDuoWithAmazonQPermissionsPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

GlobalAcceleratorFullAccess

Description : Autoriser GlobalAccelerator les utilisateurs à accéder pleinement à toutes les API

GlobalAcceleratorFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer GlobalAcceleratorFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 novembre 2018, 02:44 UTC
- Heure modifiée : 04 décembre 2020, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

GlobalAcceleratorReadOnlyAccess

Description : Autoriser GlobalAccelerator les utilisateurs à accéder aux API en lecture seule

GlobalAcceleratorReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer GlobalAcceleratorReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 novembre 2018, 02:41 UTC
- Heure modifiée : 27 novembre 2018, 02:41 UTC

- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

GreengrassOTAUpdateArtifactAccess

Description : Fournit un accès en lecture aux artefacts de mise à jour de Greengrass OTA dans toutes les régions de Greengrass

GreengrassOTAUpdateArtifactAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer GreengrassOTAUpdateArtifactAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 29 novembre 2017, 18:11 UTC
- Heure modifiée : 18 décembre 2018, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-greengrass-updates/*"
      ]
    }
  ]
}
```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

GroundTruthSyntheticConsoleFullAccess

Description : Cette politique accorde les autorisations nécessaires pour utiliser toutes les fonctionnalités de la console synthétique SageMaker Ground Truth.

GroundTruthSyntheticConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer GroundTruthSyntheticConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 août 2022, 15:58 UTC
- Heure modifiée : 25 août 2022, 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

GroundTruthSyntheticConsoleReadOnlyAccess

Description : Cette politique accorde un accès en lecture seule à SageMaker Ground Truth Synthetic via le. Console de gestion AWS

GroundTruthSyntheticConsoleReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer GroundTruthSyntheticConsoleReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 25 août 2022, 15:58 UTC

- Heure modifiée : 25 août 2022, 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

Health_OrganizationsServiceRolePolicy

Description : Politique AWS de santé pour activer la fonctionnalité d'affichage organisationnel

Health_OrganizationsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 16 décembre 2019, 13:28 UTC
- Heure modifiée : 06 février 2024, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```



```
]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

IAMAccessAdvisorReadOnly

Description : Cette politique permet de lire toutes les informations d'accès fournies par le conseiller d'accès IAM, telles que les informations relatives au dernier accès au service.

IAMAccessAdvisorReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer IAMAccessAdvisorReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 21 juin 2019, 19:33 UTC
- Heure modifiée : 21 juin 2019, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

IAMAccessAnalyzerFullAccess

Description : fournit un accès complet à IAM Access Analyzer

IAMAccessAnalyzerFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer IAMAccessAnalyzerFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 décembre 2019, 17:12 UTC
- Heure modifiée : 02 décembre 2019, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

IAMAccessAnalyzerReadOnlyAccess

Description : fournit un accès en lecture seule aux ressources d'IAM Access Analyzer

IAMAccessAnalyzerReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `IAMAccessAnalyzerReadOnlyAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 02 décembre 2019, 17:12 UTC
- Heure modifiée : 18 juillet 2024, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

IAMFullAccess

Description : fournit un accès complet à IAM via le Console de gestion AWS.

IAMFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer IAMFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 21 juin 2019, 19:40 UTC
- ARN: `arn:aws:iam::aws:policy/IAMFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

IAMReadOnlyAccess

Description : fournit un accès en lecture seule à IAM via le Console de gestion AWS.

IAMReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer IAMReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 06 février 2015, 18:40 UTC
- Heure modifiée : 25 janvier 2018, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/IAMReadOnlyAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

IAMSelfManageServiceSpecificCredentials

Description : permet à un utilisateur IAM de gérer ses propres informations d'identification spécifiques au service.

IAMSelfManageServiceSpecificCredentials est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer IAMSelfManageServiceSpecificCredentials à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 décembre 2016, 17:25 UTC
- Heure modifiée : 22 décembre 2016, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

IAMUserChangePassword

Description : permet à un utilisateur IAM de modifier son propre mot de passe.

IAMUserChangePassword est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer IAMUserChangePassword à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 15 novembre 2016, 00:25 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: arn:aws:iam::aws:policy/IAMUserChangePassword

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

IAMUserSSHKeys

Description : permet à un utilisateur IAM de gérer ses propres clés SSH.

IAMUserSSHKeys est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer IAMUserSSHKeys à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 juillet 2015, 17:08 UTC
- Heure modifiée : 09 juillet 2015, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserSSHKeys`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

IVSFullAccess

Description : fournit un accès complet au service vidéo interactif (IVS). Comprend également des autorisations pour les services dépendants, nécessaires pour un accès complet à la console IVS.

IVSFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer IVSFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 13 décembre 2023, 21:20 UTC
- Heure modifiée : 13 décembre 2023, 21:20 UTC
- ARN: `arn:aws:iam::aws:policy/IVSFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
```

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

IVSReadOnlyAccess

Description : fournit un accès en lecture seule à IVS Low-Latency et aux API de streaming Real-Time

IVSReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer IVSReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 décembre 2023, 18:00 UTC
- Heure modifiée : 25 septembre 2026, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/IVSReadOnlyAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

IVSRecordToS3

Description : Rôle lié à un service pour exécuter S3 PutObject pour enregistrer des flux en direct IVS

IVSRecordToS3 est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 05 décembre 2020, 00:10 UTC
- Heure modifiée : 05 décembre 2020, 00:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

KafkaConnectServiceRolePolicy

Description : Cette politique autorise Kafka Connect à gérer les AWS ressources en votre nom.

KafkaConnectServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 07 septembre 2021, 13:12 UTC
- Heure modifiée : 07 septembre 2021, 13:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

KafkaServiceRolePolicy

Description : Politique de rôle lié aux services IAM pour Kafka.

KafkaServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 15 novembre 2018, 23:31 UTC
- Heure modifiée : 10 novembre 2025, 23:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  }
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

KeyspacesCDCServiceRolePolicy

Description : accorde les autorisations requises à Amazon Keyspaces pour la capture des données relatives aux modifications

KeyspacesCDCServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle

- Heure de création : 21 juin 2025, 00:22 UTC
- Heure modifiée : 21 juin 2025, 00:22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/KeyspacesCDCServiceRolePolicy

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

KeyspacesReplicationServiceRolePolicy

Description : Autorisations requises par Keyspaces pour la réplication des données entre régions

KeyspacesReplicationServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 02 mai 2023, 16:15 UTC
- Heure modifiée : 15 novembre 2024, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
            ]
        }
    }
}
]

```

```
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

LakeFormationDataAccessServiceRolePolicy

Description : Politique visant à accorder un accès temporaire aux données relatives aux ressources de la formation lacustre

LakeFormationDataAccessServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 20 juin 2019, 20:46 UTC
- Heure modifiée : 06 février 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "LakeFormationDataAccessServiceRolePolicy",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets"
    ],
    "Resource" : [
      "arn:aws:s3:::*"
    ]
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

LexBotPolicy

Description : Politique relative au cas d'utilisation de AWS Lex Bot

LexBotPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 17 février 2017, 22:18 UTC
- Heure modifiée : 13 novembre 2019, 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

LexChannelPolicy

Description : Politique relative au cas d'utilisation de AWS Lex Channel

LexChannelPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 17 février 2017, 23:23 UTC
- Heure modifiée : 17 février 2017, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

LightsailExportAccess

Description : Politique de rôle liée au service AWS Lightsail qui accorde des autorisations pour exporter des ressources

LightsailExportAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 28 septembre 2018, 16:35 UTC
- Heure modifiée : 15 janvier 2022, 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

MediaConnectGatewayInstanceRolePolicy

Description : Cette politique autorise l'enregistrement d'instances de MediaConnect passerelle sur une MediaConnect passerelle.

MediaConnectGatewayInstanceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `MediaConnectGatewayInstanceRolePolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 22 mars 2023, 20:43 UTC
- Heure modifiée : 22 mars 2023, 20:43 UTC
- ARN: `arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MediaConnectGateway",
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DiscoverGatewayPollEndpoint",
        "mediaconnect:PollGateway",
        "mediaconnect:SubmitGatewayStateChange"
      ],
      "Resource" : "*"
    }
  ]
}
```


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

MediaPackageServiceRolePolicy

Description : Permet MediaPackage de publier des journaux sur CloudWatch

MediaPackageServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 18 septembre 2020, 17:45 UTC
- Heure modifiée : 18 septembre 2020, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

MemoryDBServiceRolePolicy

Description : Cette politique permet à MemoryDB de gérer les AWS ressources en votre nom si nécessaire à la gestion de vos ressources.

MemoryDBServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle

- Heure de création : 17 août 2021, 22:34 UTC
- Heure modifiée : 01 décembre 2024, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

MigrationHubDMSAccessServiceRolePolicy

Description : Politique selon laquelle le service de migration de base de données doit jouer un rôle dans le compte du client pour appeler Migration Hub

MigrationHubDMSAccessServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle

- Heure de création : 12 juin 2019, 17:50 UTC
- Heure modifiée : 07 octobre 2019, 17:57 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

MigrationHubServiceRolePolicy

Description : Permet à Migration Hub d'appeler Application Discovery Service en votre nom

MigrationHubServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 12 juin 2019, 17:22 UTC
- Heure modifiée : 06 août 2020, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
      "*"
    ]
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

MigrationHubSMSAccessServiceRolePolicy

Description : Politique selon laquelle le service de migration de serveurs doit jouer un rôle dans le compte du client pour appeler Migration Hub

MigrationHubSMSAccessServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 12 juin 2019, 18:30 UTC
- Heure modifiée : 07 octobre 2019, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

```
}  
]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

MonitronServiceRolePolicy

Description : Politique pour le rôle lié au service AWS Monitron accordant l'accès aux ressources client requises.

MonitronServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 02 mai 2022, 19:22 UTC
- Heure modifiée : 02 mai 2022, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/monitron/*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

MultiPartyApprovalFullAccess

Description : fournit un accès complet à Multi-party l'approbation. Cette politique inclut également les autorisations associées aux AWS organisations et à AWS IAM Identity pour la gestion des équipes d'approbation et des sources d'identité.

MultiPartyApprovalFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer MultiPartyApprovalFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 juin 2025, 20:22 UTC

- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/MultiPartyApprovalFullAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            }
        }
    }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

MultiPartyApprovalReadOnlyAccess

Description : fournit un accès en lecture seule à l'approbation. Multi-party Cette politique inclut également l'autorisation de lecture associée pour AWS les organisations et AWS IAM Identity pour les équipes d'approbation et les sources d'identité.

MultiPartyApprovalReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `MultiPartyApprovalReadOnlyAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 juin 2025, 20:07 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/MultiPartyApprovalReadOnlyAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"  
  }  
}  
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

NeptuneConsoleFullAccess

Description : fournit un accès complet à la gestion d'Amazon Neptune à l'aide du Console de gestion AWS. Notez que cette politique accorde également un accès complet à la publication sur toutes les rubriques SNS du compte, des autorisations pour créer et modifier des instances Amazon EC2 et des configurations VPC, des autorisations pour afficher et répertorier les clés sur Amazon KMS et un accès complet à Amazon RDS. Pour de plus amples informations, consultez <https://aws.amazon.com/neptune/faqs/>.

NeptuneConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer NeptuneConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 juin 2018, 21:35 UTC
- Heure modifiée : 30 novembre 2023, 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneConsoleFullAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "AllowOtherDependentPermissions",
    "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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

NeptuneFullAccess

Description : fournit un accès complet à Amazon Neptune. Notez que cette politique accorde également un accès complet à la publication sur toutes les rubriques SNS du compte et un accès

complet à Amazon RDS. Pour de plus amples informations, consultez <https://aws.amazon.com/neptune/faqs/>.

NeptuneFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer NeptuneFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 mai 2018, 19:17 UTC
- Heure modifiée : 22 janvier 2024, 16:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneFullAccess`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:RemoveTagsForResource",
    "rds:ResetDBClusterParameterGroup",
    "rds:ResetDBParameterGroup",
    "rds:RestoreDBClusterFromSnapshot",
    "rds:RestoreDBClusterToPointInTime",
    "rds:StartDBCluster",
    "rds:StopDBCluster"
  ],
  "Resource" : [
    "*"
  ]

```

```

    ]
  },
  {
    "Sid" : "AllowOtherDependentPermissions",
    "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" : [
        "*"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

NeptuneGraphReadOnlyAccess

Description : fournit un accès en lecture seule à toutes les ressources Amazon Neptune Analytics ainsi que des autorisations en lecture seule pour les services dépendants.

NeptuneGraphReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer NeptuneGraphReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 novembre 2023, 07:32 UTC
- Heure modifiée : 30 novembre 2023, 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:*"
    ]
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

NeptuneReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon Neptune. Notez que cette politique accorde également l'accès aux ressources Amazon RDS. Pour de plus amples informations, consultez <https://aws.amazon.com/neptune/faqs/>.

NeptuneReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer NeptuneReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 mai 2018, 19:16 UTC
- Heure modifiée : 22 janvier 2024, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "*"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)

- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

NetworkAdministrator

Description : accorde des autorisations d'accès complètes aux AWS services et aux actions nécessaires pour configurer et configurer les ressources AWS réseau.

NetworkAdministrator est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer NetworkAdministrator à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux fonctions
- Heure de création : 10 novembre 2016, 17:31 UTC
- Heure modifiée : 09 juillet 2026, 14:42 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/NetworkAdministrator`

Version de la politique

Version de la politique : v16 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            ]
        }
    }
}
]
}
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

NetworkSecurityDirectorServiceLinkedRolePolicy

Description : fournit des autorisations pour le rôle lié au service AWS Shield Network Security Director afin d'évaluer des environnements spécifiques.

NetworkSecurityDirectorServiceLinkedRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 13 juin 2025, 20:07 UTC
- Heure modifiée : 24 septembre 2026, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/NetworkSecurityDirectorServiceLinkedRolePolicy`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

NetworkSecurityManagerServiceRolePolicy

Description : Politique d'accès permettant au rôle lié à un NetworkSecurityManager service d'effectuer NetworkSecurityManager-related des actions sur NetworkSecurityManager-managed les ressources d'un client Compte AWS.

NetworkSecurityManagerServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle

- Heure de création : 18 août 2026, 18:27 UTC
- Heure modifiée : 18 août 2026, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/NetworkSecurityManagerServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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::*:vpccorigin/*"
},
{
    "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"
      }
    }
  }
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

NovaActServiceRolePolicy

Description : Cette politique permet NovaAct de créer et de gérer les ressources nécessaires au fonctionnement des agents de Nova Act.

NovaActServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 26 novembre 2025, 16:19 UTC
- Heure modifiée : 26 novembre 2025, 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/NovaActServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/NovaAct"
      }
    }
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

OAMFullAccess

Description : fournit un accès complet à CloudWatch Observability Access Manager

OAMFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer OAMFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 novembre 2022, 13:38 UTC
- Heure modifiée : 27 novembre 2022, 13:38 UTC
- ARN: `arn:aws:iam::aws:policy/OAMFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

OAMReadOnlyAccess

Description : fournit un accès en lecture seule à CloudWatch Observability Access Manager

OAMReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer OAMReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 novembre 2022, 13:29 UTC
- Heure modifiée : 27 novembre 2022, 13:29 UTC

- ARN: `arn:aws:iam::aws:policy/OAMReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

OpensearchIngestionSelfManagedVpcePolicy

Description : permet à Amazon OpenSearch Ingestion de décrire les ressources réseau et d'écrire des mesures de service dans Cloudwatch

OpensearchIngestionSelfManagedVpcePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 10 juin 2024, 19:59 UTC
- Heure modifiée : 10 juin 2024, 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/OpensearchIngestionSelfManagedVpcePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

PartnerCentralAccountManagementUserRoleAssociation

Description : Permet d'associer et de dissocier les utilisateurs centraux des partenaires dotés de rôles IAM

PartnerCentralAccountManagementUserRoleAssociation est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer PartnerCentralAccountManagementUserRoleAssociation à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 10 novembre 2023, 02:03 UTC
- Heure modifiée : 10 novembre 2023, 02:03 UTC
- ARN: `arn:aws:iam::aws:policy/PartnerCentralAccountManagementUserRoleAssociation`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

PartnerCentralIncentiveBenefitManagement

Description : La politique donne accès à la gestion de tous les avantages des incitations dans AWS Partner Central.

PartnerCentralIncentiveBenefitManagement est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer PartnerCentralIncentiveBenefitManagement à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 février 2026, 16:42 UTC
- Heure modifiée : 12 mars 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/PartnerCentralIncentiveBenefitManagement`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

PowerUserAccess

Description : fournit un accès complet aux AWS services et aux ressources, mais ne permet pas la gestion des utilisateurs et des groupes.

PowerUserAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer PowerUserAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:39 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC

- ARN: `arn:aws:iam::aws:policy/PowerUserAccess`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

PricingPlanManagerFullAccess

Description : Fournit un accès complet au AWS Pricing Plan Manager

PricingPlanManagerFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer PricingPlanManagerFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 juillet 2026, 16:42 UTC
- Heure modifiée : 30 juillet 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/PricingPlanManagerFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

PricingPlanManagerReadOnlyAccess

Description : fournit un accès en lecture seule au AWS Pricing Plan Manager

PricingPlanManagerReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer PricingPlanManagerReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 juillet 2026, 16:42 UTC
- Heure modifiée : 30 juillet 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/PricingPlanManagerReadOnlyAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ppmglobalactions",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:ListSubscriptions",
        "pricingplanmanager:GetSubscription"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

QAppsServiceRolePolicy

Description : octroie des autorisations à Amazon Q Apps Services AWS et les ressources utilisées ou gérées par Amazon Q Apps.

QAppsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 26 septembre 2024, 19:22 UTC
- Heure modifiée : 26 septembre 2024, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/QAppsServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QAppsPutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
    "StringEquals" : {
      "cloudwatch:namespace" : "AWS/QApps"
    }
  }
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

QBusinessQuicksightPluginPolicy

Description : accorde à QBusiness l'autorisation d'appeler QuickSight des API pour le plugin QuickSight

QBusinessQuicksightPluginPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer QBusinessQuicksightPluginPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 03 décembre 2024, 15:36 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/QBusinessQuicksightPluginPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QBusinessToQuickSightPredictQAResultsInvocation",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:PredictQAResults"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:topic/*",
        "arn:aws:quicksight:*:*:dashboard/*"
      ]
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

QBusinessServiceRolePolicy

Description : accorde des autorisations Services AWS et des ressources utilisées ou gérées par Amazon Q

QBusinessServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 29 avril 2024, 16:05 UTC
- Heure modifiée : 29 avril 2024, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/QBusinessServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

Description : Politique utilisée par QuickSight l'équipe pour accéder aux données clients produites par S3 Storage Management Analytics.

QuickSightAccessForS3StorageManagementAnalyticsReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer QuickSightAccessForS3StorageManagementAnalyticsReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 12 juin 2017, 18:18 UTC
- Heure modifiée : 08 octobre 2019, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

RDSCloudHsmAuthorizationRole

Description : Politique par défaut pour le rôle de service Amazon RDS.

RDSCloudHsmAuthorizationRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer RDSCloudHsmAuthorizationRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 26 septembre 2019, 22:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm>DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ReadOnlyAccess

Description : fournit un accès en lecture seule aux AWS services et ressources.

ReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:39 UTC
- Heure modifiée : 24 septembre 2026, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/ReadOnlyAccess`

Version de la politique

Version de la politique : v190 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:ListGroup",
"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",
"qlldb:DescribeJournalKinesisStream",
"qlldb:DescribeJournalS3Export",
"qlldb:DescribeLedger",
"qlldb:GetBlock",
"qlldb:GetDigest",
"qlldb:GetRevision",
"qlldb:ListJournalKinesisStreamsForLedger",
"qlldb:ListJournalS3Exports",
"qlldb:ListJournalS3ExportsForLedger",
"qlldb:ListLedgers",
"qlldb: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:DescribeSenderId",
"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"
    }
  }
}
]

```



```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ReInventTicketApprovalAccess

Description : accorde à un rôle IAM ou à un utilisateur un accès complet pour consulter les détails des frais de re:Invent Pass et approuver la facturation sur ses comptes AWS

ReInventTicketApprovalAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ReInventTicketApprovalAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 10 juin 2026, 18:57 UTC
- Heure modifiée : 10 juin 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/ReInventTicketApprovalAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowBillToAWSActions",
      "Effect" : "Allow",
      "Action" : [
        "eventsbilltoaws:info",
        "eventsbilltoaws:approve"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ResourceGroupsandTagEditorFullAccess

Description : fournit un accès complet aux groupes de ressources et à l'éditeur de balises.

ResourceGroupsandTagEditorFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ResourceGroupsandTagEditorFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée

- Heure de création : 06 février 2015, 18:39 UTC
- Heure modifiée : 10 août 2023, 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ResourceGroupsandTagEditorReadOnlyAccess

Description : permet d'utiliser les groupes de ressources et l'éditeur de balises, mais n'autorise pas la modification des balises via l'éditeur de balises.

ResourceGroupsandTagEditorReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ResourceGroupsandTagEditorReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:39 UTC
- Heure modifiée : 10 août 2023, 13:42 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ResourceGroupsServiceRolePolicy

Description : permet aux groupes de AWS ressources d'interroger les AWS services qui possèdent vos ressources afin de maintenir le groupe à jour

ResourceGroupsServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 05 janvier 2023, 16:57 UTC
- Heure modifiée : 05 janvier 2023, 16:57 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/ResourceGroupsServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ResourceGroupsTaggingAPITagUntagSupportedResources

Description : fournit des autorisations pour baliser et débaliser toutes les ressources prises en charge par l'API de balisage des groupes de ressources. Cette politique accorde également les autorisations nécessaires pour récupérer toutes les ressources balisées ou précédemment balisées via l'API de balisage des groupes de ressources.

ResourceGroupsTaggingAPITagUntagSupportedResources est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ResourceGroupsTaggingAPITagUntagSupportedResources à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 octobre 2024, 11:11 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsTaggingAPITagUntagSupportedResources`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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",
"qlldb:TagResource",
"qlldb: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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ROSAAmazonEBSCSIDriverOperatorPolicy

Description : Permet à l'opérateur du pilote OpenShift Amazon EBS Container Storage Interface (CSI) d'installer et de gérer le pilote Amazon EBS CSI sur un cluster Red Hat OpenShift Service on AWS (ROSA). Le pilote Amazon EBS CSI permet aux clusters ROSA de gérer le cycle de vie des volumes Amazon EBS pour les volumes persistants.

ROSAAmazonEBSCSIDriverOperatorPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ROSAAmazonEBSCSIDriverOperatorPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- **Type** : Politique relative aux rôles de service
- **Heure de création** : 20 avril 2023, 22:36 UTC
- **Heure modifiée** : 19 août 2026, 05:07 UTC
- **ARN**: `arn:aws:iam::aws:policy/service-role/ROSAAmazonEBSCSIDriverOperatorPolicy`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
```

```
    "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" : "CreateVolumesFromAndEnableFSR0nManagedSnapshots",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateVolume",
      "ec2:EnableFastSnapshotRestores"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "StringEquals" : {
```

```
        "aws:ResourceTag/red-hat-managed" : "true"
    }
}
},
{
    "Sid" : "CreateVolumesFromAndEnableFSR0nUserBroughtSnapshots",
    "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:eks: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"
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ROSACloudNetworkConfigOperatorPolicy

Description : Permet à l'opérateur du OpenShift Cloud Network Config Controller de provisionner et de gérer les ressources réseau destinées à être utilisées par la superposition réseau du cluster Red Hat OpenShift Service on AWS (ROSA). L'opérateur de réseau OpenShift cloud interagit avec les AWS API pour le compte des plugins réseau via CustomResourceDefinitions. L'opérateur utilise ces autorisations de politique pour gérer les adresses IP privées des instances Amazon EC2 dans le cadre du cluster ROSA.

ROSACloudNetworkConfigOperatorPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ROSACloudNetworkConfigOperatorPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 20 avril 2023, 22:34 UTC
- Heure modifiée : 20 avril 2023, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ROSAControlPlaneOperatorPolicy

Description : permet à Red Hat OpenShift Service on AWS (ROSA) de gérer les ressources Amazon EC2 et Amazon Route 53 du cluster ROSA.

R0SAControlPlaneOperatorPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer R0SAControlPlaneOperatorPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 24 avril 2023 à 23:02 UTC
- Heure modifiée : 28 juillet 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/R0SAControlPlaneOperatorPolicy`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ROSAImageRegistryOperatorPolicy

Description : permet à l'opérateur du registre OpenShift d'images de provisionner et de gérer les compartiments et les objets Amazon S3 à utiliser par le registre d'images intégré au cluster Red Hat OpenShift Service on AWS (ROSA) afin de répondre aux exigences de stockage ROSA. L'opérateur de registre d' OpenShift images installe et gère le registre interne d'un OpenShift cluster Red Hat.

ROSAImageRegistryOperatorPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `R0SAImageRegistryOperatorPolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 27 avril 2023, 20:13 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/R0SAImageRegistryOperatorPolicy`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}/*"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ROSAIngressOperatorPolicy

Description : Permet à l'opérateur d' OpenShift entrée de provisionner et de gérer les équilibres de charge et les configurations du système de noms de domaine (DNS) pour les clusters Red Hat OpenShift Service on AWS (ROSA). La politique autorise l'accès en lecture aux valeurs des balises, que l'opérateur filtre pour les ressources Route 53 afin de découvrir les zones hébergées.

ROSAIngressOperatorPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ROSAIngressOperatorPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 20 avril 2023, 22:37 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ROSAInstallerPolicy

Description : permet au programme d'installation de Red Hat OpenShift Service on AWS (ROSA) de gérer les AWS ressources qui prennent en charge l'installation du cluster ROSA. Cela inclut la gestion des profils d'instance pour les nœuds de travail ROSA.

ROSAInstallerPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ROSAInstallerPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 06 juin 2023, 21:00 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy`

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ROSAKarpenterControllerPolicy

Description : Fournit des autorisations permettant au contrôleur ROSA Karpenter de manière dynamique de provisionner et de gérer des instances EC2 pour Red Hat OpenShift Service sur des clusters de plans de contrôle hébergés AWS (ROSA). Cela inclut la gestion du cycle de vie de la flotte et des instances EC2, les requêtes relatives à la tarification des instances, les opérations KMS pour le chiffrement des volumes EBS avec des clés gérées par le client et la gestion des profils d'instance IAM.

ROSAKarpenterControllerPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ROSAKarpenterControllerPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 27 juillet 2026, 16:42 UTC
- Heure modifiée : 27 juillet 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKarpenterControllerPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ROSAKMSPProviderPolicy

Description : permet au fournisseur de AWS chiffrement ROSA intégré de gérer les AWS clés du service de gestion des clés (KMS) pour prendre en charge le chiffrement des données etcd à l'aide d'une clé AWS KMS fournie par le client. La politique autorise le chiffrement et le déchiffrement des données à l'aide de clés KMS.

ROSAKMSPProviderPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ROSAKMSPProviderPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 27 avril 2023, 20:10 UTC
- Heure modifiée : 27 avril 2023, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKMSPProviderPolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ROSAKubeControllerPolicy

Description : Permet au contrôleur ROSA Kubernetes de gérer les ressources Amazon EC2, Elastic Load Balancing (ELB) et AWS Key Management Service (KMS) pour un cluster ROSA.

ROSAKubeControllerPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ROSAKubeControllerPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 27 avril 2023, 20:09 UTC
- Heure modifiée : 17 septembre 2026, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy`

Version de la politique

Version de la politique : v8 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "LoadBalancerManagement",
    "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" : "LoadBalancerManagementResourceTag",
        "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"
        }
    }
}

```

```
}  
  }  
    }  
      ]  
    }  
  }
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ROSAManageSubscription

Description : Cette politique fournit les autorisations nécessaires pour gérer l'abonnement Red Hat OpenShift Service on AWS (ROSA).

ROSAManageSubscription est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ROSAManageSubscription à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Temps de création : 11 avril 2022, 20:58 UTC
- Heure modifiée : 04 août 2023, 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/ROSAManageSubscription`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ROSANodePoolManagementPolicy

Description : Permet à Red Hat OpenShift Service on AWS (ROSA) de gérer les instances EC2 du cluster en tant que nœuds de travail, y compris l'autorisation de configurer des groupes de sécurité et de baliser des instances et des volumes. Cette politique autorise également l'utilisation d'instances EC2 avec un chiffrement de disque fourni par les clés du service de gestion des AWS clés (KMS).

ROSANodePoolManagementPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ROSANodePoolManagementPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 08 juin 2023, 20:48 UTC
- Heure modifiée : 29 juillet 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  }
}
```

```
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ROSASharedVPCEndpointPolicy

Description : permet au programme d'installation de Red Hat OpenShift Service on AWS (ROSA) de configurer les points de terminaison et les groupes de sécurité VPC. Destiné à être utilisé sur un VPC partagé.

ROSASharedVPCEndpointPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ROSASharedVPCEndpointPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 août 2025, 17:19 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/ROSASharedVPCEndpointPolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      ]
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ROSASharedVPCRoute53Policy

Description : permet au programme d'installation de Red Hat OpenShift Service on AWS (ROSA) de configurer les enregistrements Route53. Destiné à être utilisé sur un VPC partagé.

ROSASharedVPCRoute53Policy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ROSASharedVPCRoute53Policy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 11 août 2025, 17:19 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/ROSASharedVPCRoute53Policy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ROSASRESupportPolicy

Description : fournit à l'ingénierie de fiabilité des sites ROSA (SRE) les autorisations nécessaires pour observer, diagnostiquer et prendre en charge initialement les AWS ressources associées aux clusters Red Hat OpenShift Service on AWS (ROSA), y compris la possibilité de modifier l'état du nœud du cluster ROSA.

ROSASRESupportPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ROSASRESupportPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 01 juin 2023, 14:36 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "DescribeIAMRoles",
    "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"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ROSASWorkerInstancePolicy

Description : autorise les nœuds de travail Red Hat OpenShift Service on AWS (ROSA) de votre compte à accéder en lecture seule aux instances Amazon EC2 et à la gestion du cycle de vie Régions AWS des nœuds de calcul.

ROSASWorkerInstancePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ROSASWorkerInstancePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 20 avril 2023, 22:35 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  }
}
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

Route53RecoveryReadinessServiceRolePolicy

Description : Politique de rôle lié aux services pour la préparation à la reprise de la Route 53

Route53RecoveryReadinessServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 15 juillet 2021, 16:06 UTC
- Heure modifiée : 14 février 2023, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

Route53ResolverServiceRolePolicy

Description : Permet l'accès aux Services AWS ressources utilisées ou gérées par Route53 Resolver

Route53ResolverServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 12 août 2020, 17:47 UTC
- Heure modifiée : 12 août 2020, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

RTBFabricServiceRolePolicy

Description : rôle lié à un service requis pour que AWS RTBfabric crée et gère les ressources de votre interface réseau et fournisse des métriques.

RTBFabricServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 16 octobre 2025, 16:49 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/RTBFabricServiceRolePolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

S3StorageLensServiceRolePolicy

Description : Permet d'accéder à S3 Storage Lens Services AWS et aux ressources utilisées ou gérées par S3 Storage Lens

S3StorageLensServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 18 novembre 2020, 18:15 UTC
- Heure modifiée : 18 novembre 2020, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioAdminIAMConsolePolicy

Description : fournit des privilèges administratifs initiaux et de configuration individuelle pour Amazon SageMaker Unified Studio via le SDK Console de gestion AWS et. Permet de lancer SageMaker Unified Studio Portal.

SageMakerStudioAdminIAMConsolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioAdminIAMConsolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 août 2025, 22:49 UTC
- Heure modifiée : 26 août 2026, 22:47 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminIAMConsolePolicy`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioAdminIAMDefaultExecutionPolicy

Description : Politique d'exécution administrative pour l'utilisation des rôles IAM avec SageMaker Unified Studio. Permet aux administrateurs de provisionner, de gérer et d'accéder aux ressources de votre compte (à l'exception de l'accès aux ressources de données) pour IAM-based l'utilisation d' SageMaker Unified Studio.

SageMakerStudioAdminIAMDefaultExecutionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `SageMakerStudioAdminIAMDefaultExecutionPolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 août 2025, 17:19 UTC
- Heure modifiée : 14 juillet 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminIAMDefaultExecutionPolicy`

Version de la politique

Version de la politique : v24 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/
AWSServiceRoleForAmazonMWA",
    "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" : "AirflowMWSAA",
  "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:*",
      "extract:*",
      "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:*"
    ]
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioAdminIAMPermissiveExecutionPolicy

Description : Politique d'exécution administrative pour l'utilisation des rôles IAM avec SageMaker Unified Studio. Permet aux administrateurs de provisionner, de gérer et d'accéder aux ressources du compte local (y compris un accès étendu à toutes les API des services de données tels que S3, Glue, CloudWatch Logs, etc.) pour IAM-based utiliser SageMaker Unified Studio.

SageMakerStudioAdminIAMPermissiveExecutionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioAdminIAMPermissiveExecutionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 août 2025, 17:19 UTC
- Heure modifiée : 14 juillet 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminIAMPermissiveExecutionPolicy`

Version de la politique

Version de la politique : v21 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/
AWSServiceRoleForAmazonMWSAA",
      "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAAServerless",
      "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"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioAdminProjectUserRolePolicy

Description : Cette politique IAM accorde à un rôle IAM un accès complet à AWS Glue Data Catalog (métadonnées) et à Amazon S3 (données réelles) pour les opérations des lacs de données, avec un accès limité par compte et par balises de rôle.

SageMakerStudioAdminProjectUserRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioAdminProjectUserRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 juillet 2025, 20:52 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminProjectUserRolePolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioBedrockAgentServiceRolePolicy

Description : permet aux agents Amazon Bedrock d'accéder aux modèles Amazon Bedrock et à d'autres ressources associées à un agent dans SageMaker Studio.

SageMakerStudioBedrockAgentServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioBedrockAgentServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- **Type** : Politique relative aux rôles de service
- **Heure de création** : 13 février 2025, 23:37 UTC
- **Heure modifiée** : 12 février 2026, 18:00 UTC
- **ARN**: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockAgentServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}/*"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioBedrockChatAgentUserRolePolicy

Description : Permet d'accéder à la configuration de l'application d'agent de chat Amazon Bedrock et à l'agent Amazon Bedrock dans SageMaker Studio.

SageMakerStudioBedrockChatAgentUserRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioBedrockChatAgentUserRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 13 février 2025, 23:52 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockChatAgentUserRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}/*"
            ]
        }
    }
}
}

```

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioBedrockEvaluationJobServiceRolePolicy

Description : permet à Amazon Bedrock d'accéder aux modèles et aux ensembles de données Amazon Bedrock pour les tâches d'évaluation dans Studio. SageMaker

SageMakerStudioBedrockEvaluationJobServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioBedrockEvaluationJobServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 14 février 2025, 00:37 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockEvaluationJobServiceRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}/*"
            ]
        }
    }
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioBedrockFlowServiceRolePolicy

Description : permet à Amazon Bedrock Flows d'accéder aux modèles Amazon Bedrock et à d'autres ressources associées à un flux dans SageMaker Studio.

SageMakerStudioBedrockFlowServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioBedrockFlowServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 14 février 2025, 00:07 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockFlowServiceRolePolicy`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioBedrockFunctionExecutionRolePolicy

Description : permet à AWS Lambda d'accéder à la configuration d'un composant de fonction Amazon Bedrock dans SageMaker Studio.

SageMakerStudioBedrockFunctionExecutionRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioBedrockFunctionExecutionRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 25 février 2025, 03:52 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockFunctionExecutionRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy

Description : permet de configurer des magasins vectoriels et des bases de connaissances Amazon Bedrock dans SageMaker Studio.

SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 25 février 2025, 03:37 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
      }
    }
  ]
}
```

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy

Description : permet aux bases de connaissances Amazon Bedrock d'accéder aux modèles et aux sources de données Amazon Bedrock dans SageMaker Studio.

SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 25 février 2025, 02:52 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioBedrockPromptUserRolePolicy

Description : Permet d'accéder à une invite Amazon Bedrock et à sa configuration dans SageMaker Studio.

SageMakerStudioBedrockPromptUserRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `SageMakerStudioBedrockPromptUserRolePolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 14 février 2025, 00:22 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockPromptUserRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}/*"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioDomainExecutionRolePolicy

Description : Cette politique est utilisée par Amazon SageMaker Studio pour cataloguer, découvrir, gérer, partager et analyser les données du domaine Amazon SageMaker Studio.

SageMakerStudioDomainExecutionRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioDomainExecutionRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 20 novembre 2024, 21:56 UTC
- Heure modifiée : 12 août 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioDomainExecutionRolePolicy`

Version de la politique

Version de la politique : v23 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/*"
```

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioDomainServiceRolePolicy

Description : rôle de service pour les actions au niveau du domaine sur le portail effectuées par Amazon SageMaker Studio.

SageMakerStudioDomainServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioDomainServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 20 novembre 2024, 21:56 UTC
- Heure modifiée : 20 novembre 2024, 21:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioDomainServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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*"
        }
      }
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioEMRContainersSystemNamespaceRolePolicy

Description : Amazon SageMaker Studio crée des rôles IAM pour que les utilisateurs des projets puissent effectuer des actions d'analyse de données, d'intelligence artificielle et d'apprentissage automatique, et utilise cette politique lors de la création de ces rôles afin de définir les autorisations liées à l'EMR.

SageMakerStudioEMRContainersSystemNamespaceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioEMRContainersSystemNamespaceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 23 octobre 2025, 18:34 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRContainersSystemNamespaceRolePolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  }
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioEMRInstanceRolePolicy

Description : Amazon SageMaker Studio crée des rôles IAM pour que les utilisateurs des projets puissent effectuer des actions d'analyse de données, d'intelligence artificielle et d'apprentissage automatique, et utilise cette politique lors de la création de ces rôles afin de définir les autorisations liées à l'EMR.

SageMakerStudioEMRInstanceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioEMRInstanceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 27 février 2025, 00:22 UTC
- Heure modifiée : 01 juin 2026, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRInstanceRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioEMRServiceRolePolicy

Description : Amazon SageMaker Studio crée des rôles IAM pour que les utilisateurs des projets puissent effectuer des actions d'analyse de données, d'intelligence artificielle et d'apprentissage automatique, et utilise cette politique lors de la création de ces rôles afin de définir les autorisations liées à l'EMR.

SageMakerStudioEMRServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioEMRServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 31 janvier 2025, 19:52 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRServiceRolePolicy`

Version de la politique

Version de la politique : v9 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioFullAccess

Description : Cette politique fournit un accès complet à Amazon SageMaker Unified Studio via la console SageMaker de gestion Amazon.

SageMakerStudioFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 28 novembre 2024, 00:06 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioFullAccess`

Version de la politique

Version de la politique : v15 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
```

```
        "*"
    ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioProjectProvisioningRolePolicy

Description : Amazon SageMaker Studio utilise cette politique pour provisionner et gérer les ressources de votre compte.

SageMakerStudioProjectProvisioningRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioProjectProvisioningRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 20 novembre 2024, 21:58 UTC
- Heure modifiée : 22 septembre 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioProjectProvisioningRolePolicy`

Version de la politique

Version de la politique : v83 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
        "arn:aws:kms::*:key/*"
    ]
}
```

```

    "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:CreateVPCCConnection",
      "quicksight>DeleteDataSource",
      "quicksight>DeleteFolder",
      "quicksight:DescribeDataSource",
      "quicksight:DescribeFolderPermissions",
      "quicksight:DescribeDataSourcePermissions",
      "quicksight>DeleteVPCCConnection",
      "quicksight:ListFolderMembers",
      "quicksight:ListTagsForResource",
      "quicksight:UpdateDataSource",
      "quicksight:UpdateDataSourcePermissions",
      "quicksight:UpdateFolder",
      "quicksight:UpdateFolderPermissions",
      "quicksight:UpdateVPCCConnection"
    ],
    "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"
    ]
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioProjectRoleMachineLearningPolicy

Description : Amazon SageMaker Studio crée des rôles IAM pour que les utilisateurs des projets puissent effectuer des actions d'analyse de données, d'intelligence artificielle et d'apprentissage automatique, et utilise cette politique lors de la création de ces rôles afin de définir les autorisations associées. SageMaker

SageMakerStudioProjectRoleMachineLearningPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioProjectRoleMachineLearningPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 novembre 2024, 21:55 UTC
- Heure modifiée : 14 septembre 2026, 20:37 UTC

- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectRoleMachineLearningPolicy`

Version de la politique

Version de la politique : v44 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/AWSServiceRoleForAmazonMWAAAServerless"
    ]
},
{
    "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}"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioProjectUserRolePermissionsBoundary

Description : Amazon SageMaker crée des rôles IAM pour que les utilisateurs de Projects puissent effectuer des actions d'analyse de données, d'intelligence artificielle et d'apprentissage automatique, et utilise cette politique lors de la création de ces rôles afin de définir les limites de leurs autorisations.

SageMakerStudioProjectUserRolePermissionsBoundary est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioProjectUserRolePermissionsBoundary à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 novembre 2024, 21:57 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePermissionsBoundary`

Version de la politique

Version de la politique : v19 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:user}"
        }
    }
},
{
    "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" : "RedshiftServerlessCredentialsForManagedWorkgroup",
    "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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioProjectUserRolePolicy

Description : Amazon SageMaker Studio crée des rôles IAM pour que les utilisateurs des projets puissent effectuer des actions d'analyse de données, d'intelligence artificielle et d'apprentissage automatique, et utilise cette politique lors de la création de ces rôles pour définir les autorisations.

SageMakerStudioProjectUserRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioProjectUserRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 20 novembre 2024, 21:59 UTC
- Heure modifiée : 27 août 2026, 20:57 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePolicy`

Version de la politique

Version de la politique : v75 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "${aws:PrincipalAccount}"
    },
    "StringLike" : {
      "kms:ViaService" : [
        "codecommit.*.amazonaws.com"
      ]
    }
  },
  {
    "Sid" : "CodeWhisperer",
    "Effect" : "Allow",
    "Action" : [
      "codewhisperer:GenerateRecommendations"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowGlueCreateEni",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "Null" : {
        "aws:TagKeys" : "true"
      },
      "StringEquals" : {
        "glue:RoleAssumedBy" : "glue.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "GlueENISG",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface"
    ],
    "Resource" : "arn:aws:ec2:*:*:security-group/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${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/EnableAmazonBedrockIDEPPermissions" : "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/EnableAmazonBedrockIDEPPermissions" : "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/EnableAmazonBedrockIDEPpermissions" : "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}"
        }
    }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioQueryExecutionRolePolicy

Description : Amazon SageMaker Studio utilise cette politique lors de l'exécution de requêtes sur des connexions fédérées.

SageMakerStudioQueryExecutionRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `SageMakerStudioQueryExecutionRolePolicy` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 31 janvier 2025, 19:52 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioQueryExecutionRolePolicy`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioUserIAMConsolePolicy

Description : fournit des privilèges de configuration individuels pour Amazon SageMaker Unified Studio via le SDK Console de gestion AWS et. Permet de lancer SageMaker Unified Studio Portal.

SageMakerStudioUserIAMConsolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioUserIAMConsolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 août 2025, 22:49 UTC
- Heure modifiée : 31 mars 2026, 21:12 UTC
- ARN: arn:aws:iam::aws:policy/SageMakerStudioUserIAMConsolePolicy

Version de la politique

Version de la politique : v10 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
    }
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioUserIAMDefaultExecutionPolicy

Description : Politique d'exécution pour l'utilisation des rôles IAM avec SageMaker Unified Studio. Permet aux utilisateurs d'accéder aux ressources du compte local (à l'exclusion de l'accès aux ressources de données) IAM-based pour utiliser SageMaker Unified Studio.

SageMakerStudioUserIAMDefaultExecutionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioUserIAMDefaultExecutionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 août 2025, 17:19 UTC
- Heure modifiée : 13 août 2026, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioUserIAMDefaultExecutionPolicy`

Version de la politique

Version de la politique : v29 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SageMakerStudioUserIAMPermissiveExecutionPolicy

Description : Politique d'exécution pour l'utilisation des rôles IAM avec SageMaker Unified Studio. Permet aux utilisateurs d'accéder aux ressources de votre compte (y compris un accès étendu à toutes les API des services de données tels que S3, Glue, CloudWatch Logs, etc.) IAM-based pour utiliser SageMaker Unified Studio.

SageMakerStudioUserIAMPermissiveExecutionPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SageMakerStudioUserIAMPermissiveExecutionPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 18 août 2025, 17:19 UTC
- Heure modifiée : 13 août 2026, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioUserIAMPermissiveExecutionPolicy`

Version de la politique

Version de la politique : v24 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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/
AWSServiceRoleForAmazonMWAA Serverless",
        "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/*"
    ]
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SecretsManagerReadWrite

Description : Permet read/write d'accéder à AWS Secrets Manager via le Console de gestion AWS.

Remarque : cela exclut les actions IAM, à combiner avec IAMFullAccess si une configuration de rotation est requise.

SecretsManagerReadWrite est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SecretsManagerReadWrite à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 04 avril 2018, 18:05 UTC
- Heure modifiée : 25 août 2026, 23:37 UTC
- ARN: `arn:aws:iam::aws:policy/SecretsManagerReadWrite`

Version de la politique

Version de la politique : v6 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        ]
      }
    }
  }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SecurityAgentWebAppAPIPolicy

Description : autorise les utilisateurs authentifiés à accéder à l'application Web Security Agent pour configurer et exécuter des tests d'intrusion de sécurité automatisés. Cette politique permet aux

utilisateurs de gérer les pentests, de consulter les résultats, de surveiller l'exécution des tests et d'interagir avec les AWS ressources nécessaires aux opérations de tests de sécurité.

SecurityAgentWebAppAPIPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SecurityAgentWebAppAPIPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 02 décembre 2025, 15:04 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SecurityAgentWebAppAPIPolicy`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SecurityAgentWebAppPolicy

Description : autorise les utilisateurs authentifiés à accéder à l'application Web Security Agent pour configurer et exécuter des tests d'intrusion de sécurité automatisés. Cette politique permet aux utilisateurs de gérer les pentests, de consulter les résultats, de surveiller l'exécution des tests et d'interagir avec les AWS ressources nécessaires aux opérations de tests de sécurité.

SecurityAgentWebAppPolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SecurityAgentWebAppPolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 05 février 2026, 20:19 UTC
- Heure modifiée : 12 février 2026, 18:01 UTC
- ARN: arn:aws:iam::aws:policy/SecurityAgentWebAppPolicy

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
    }
  }
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SecurityAudit

Description : le modèle d'audit de sécurité donne accès à la lecture des métadonnées de configuration de sécurité. Il est utile pour les logiciels qui audient la configuration d'un Compte AWS.

SecurityAudit est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SecurityAudit à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 30 septembre 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/SecurityAudit`

Version de la politique

Version de la politique : v94 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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",
"qlldb:DescribeJournalS3Export",
"qlldb:DescribeLedger",
"qlldb:ListJournalS3Exports",
"qlldb:ListJournalS3ExportsForLedger",
"qlldb: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"
  ]
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SecurityLakeResourceManagementServiceRolePolicy

Description : Permet d'accéder à la gestion des ressources créées par Security Lake.

SecurityLakeResourceManagementServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 14 novembre 2024, 22:10 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeResourceManagementServiceRolePolicy`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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}"
        }
    }
}
]
}

```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SecurityLakeServiceLinkedRole

Description : Cette politique accorde l'autorisation d'exploiter le service Amazon Security Lake en votre nom

SecurityLakeServiceLinkedRole est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 29 novembre 2022, 14:03 UTC
- Heure modifiée : 15 juillet 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
          ]
        }
      }
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ServerMigration_ServiceRole

Description : Autorisations permettant au service de migration de AWS serveurs de migrer des machines virtuelles vers EC2 : autorise le service de migration de serveurs à placer les ressources migrées sur le compte EC2 du client.

ServerMigration_ServiceRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ServerMigration_ServiceRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service

- Heure de création : 11 août 2020, 20:41 UTC
- Heure modifiée : 15 octobre 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*/*"
        }
    }
}
]

```

```
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ServerMigrationConnector

Description : autorisations permettant au connecteur de migration de AWS serveurs de migrer des machines virtuelles vers EC2. Permet la communication avec le service de migration de AWS serveurs, l' read/write accès aux compartiments S3 commençant par « sms-b- » et « import-to-ec2- » ainsi qu'aux compartiments utilisés pour la mise à niveau du connecteur de migration de serveur, l'enregistrement du connecteur de migration de AWS serveur auprès de et le AWS téléchargement de métriques vers. AWS AWS

ServerMigrationConnector est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ServerMigrationConnector à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 octobre 2016, 21:45 UTC
- Heure modifiée : 24 octobre 2016, 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationConnector`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ServerMigrationServiceConsoleFullAccess

Description : autorisations requises pour utiliser toutes les fonctionnalités de la console du service de migration de serveurs

ServerMigrationServiceConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer `ServerMigrationServiceConsoleFullAccess` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 09 mai 2020, 17:18 UTC
- Heure modifiée : 20 juillet 2020, 22:00 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
```

```
}  
]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ServerMigrationServiceLaunchRole

Description : autorisations permettant au service de migration de AWS serveurs de créer et de mettre à jour AWS des ressources pertinentes dans celles du client Compte AWS pour le lancement de serveurs et d'applications migrés.

ServerMigrationServiceLaunchRole est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ServerMigrationServiceLaunchRole à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 26 novembre 2018, 19:53 UTC
- Heure modifiée : 15 octobre 2020, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
            }
        }
    }
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ServerMigrationServiceRoleForInstanceValidation

Description : Autorisations permettant au AWS SMS d'exécuter le script de validation des données utilisées et de success/failure renvoyer le script au SMS

ServerMigrationServiceRoleForInstanceValidation est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ServerMigrationServiceRoleForInstanceValidation à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 20 juillet 2020, 22:25 UTC
- Heure modifiée : 20 juillet 2020, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/**"
```

```
    },  
    {  
      "Effect" : "Allow",  
      "Action" : "sms:NotifyAppValidationOutput",  
      "Resource" : "*"   
    }  
  ]  
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ServiceQuotasFullAccess

Description : Fournit un accès complet aux quotas de service

ServiceQuotasFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ServiceQuotasFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 juin 2019, 15:44 UTC
- Heure modifiée : 04 février 2021, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ServiceQuotasReadOnlyAccess

Description : fournit un accès en lecture seule aux quotas de service

ServiceQuotasReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ServiceQuotasReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 24 juin 2019, 15:31 UTC
- Heure modifiée : 12 février 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess`

Version de la politique

Version de la politique : v5 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ServiceQuotasServiceRolePolicy

Description : autorise Service Quotas à créer des dossiers d'assistance en votre nom

ServiceQuotasServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 22 mai 2019, 20:44 UTC
- Heure modifiée : 24 juin 2019, 14:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
```

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

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SignInLocalDevelopmentAccess

Description : fournit des autorisations pour l'accès par programmation AWS via le AWS Sign-in service, y compris la création de jetons OAuth2 pour les outils et applications de développement.

SignInLocalDevelopmentAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SignInLocalDevelopmentAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 19 novembre 2025, 18:34 UTC
- Heure modifiée : 12 février 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/SignInLocalDevelopmentAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "signin:AuthorizeOAuth2Access",
        "signin:CreateOAuth2Token"
      ],
      "Resource" : "arn:aws:signin:*:*:oauth2/public-client/*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SimpleWorkflowFullAccess

Description : fournit un accès complet au service de configuration Simple Workflow.

SimpleWorkflowFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SimpleWorkflowFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 06 février 2015, 18:41 UTC
- Heure modifiée : 06 février 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/SimpleWorkflowFullAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SMSVoiceServiceRolePolicy

Description : Permet à SMSVoice de publier des CloudWatch statistiques en votre nom

SMSVoiceServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 14 novembre 2024, 17:04 UTC
- Heure modifiée : 14 novembre 2024, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SMSVoiceServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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

```
}  
]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SplitCostAllocationDataServiceRolePolicy

Description : autorise les données de répartition des coûts fractionnés pour récupérer AWS les informations des organisations, le cas échéant, et collecter des données de télémétrie pour les services de données de répartition des coûts fractionnés auxquels le client a opté.

SplitCostAllocationDataServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 16 avril 2024, 16:05 UTC
- Heure modifiée : 16 avril 2024, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SplitCostAllocationDataServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SSMQuickSetupRolePolicy

Description : fournit les autorisations nécessaires pour vérifier l'état de la configuration de Quick Setup, garantir une utilisation cohérente des paramètres et des ressources provisionnées, et corriger les ressources lorsqu'une dérive est détectée.

SSMQuickSetupRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 25 juin 2024, 15:20 UTC
- Heure modifiée : 18 novembre 2024, 13:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SSMQuickSetupRolePolicy`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : [
      "*"
    ]
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SupportUser

Description : Cette politique accorde des autorisations pour dépanner et résoudre les problèmes dans un Compte AWS. Cette politique permet également à l'utilisateur de contacter le AWS support pour créer et gérer des dossiers.

SupportUser est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SupportUser à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux fonctions
- Heure de création : 10 novembre 2016, 17:21 UTC
- Heure modifiée : 12 février 2026, 18:03 UTC
- ARN: arn:aws:iam::aws:policy/job-function/SupportUser

Version de la politique

Version de la politique : v11 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

SystemAdministrator

Description : octroie les autorisations d'accès complètes nécessaires aux ressources requises pour les opérations d'application et de développement.

SystemAdministrator est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer SystemAdministrator à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux fonctions
- Heure de création : 10 novembre 2016, 17:23 UTC
- Heure modifiée : 12 février 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SystemAdministrator`

Version de la politique

Version de la politique : v12 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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:ReportInstanceState",
"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"
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

TranslateFullAccess

Description : fournit un accès complet à Amazon Translate.

TranslateFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer TranslateFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 27 novembre 2018, 23:36 UTC
- Heure modifiée : 08 janvier 2020, 21:22 UTC

- ARN: `arn:aws:iam::aws:policy/TranslateFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

TranslateReadOnly

Description : fournit un accès en lecture seule à Amazon Translate.

TranslateReadOnly est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer TranslateReadOnly à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2017, 18:22 UTC
- Heure modifiée : 24 mai 2023, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateReadOnly`

Version de la politique

Version de la politique : v7 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
}
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

ViewOnlyAccess

Description : Cette politique autorise l'affichage des ressources et des métadonnées de base pour tous les AWS services.

ViewOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer ViewOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux fonctions du poste
- Heure de création : 10 novembre 2016, 17:20 UTC
- Heure modifiée : 30 septembre 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/ViewOnlyAccess`

Version de la politique

Version de la politique : v46 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  ]
}
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

VMImportExportRoleForAWSConnector

Description : Politique par défaut pour le rôle de Import/Export service de machine virtuelle, pour les clients utilisant le AWS connecteur. Le Import/Export service VM joue un rôle dans le cadre de cette politique pour répondre aux demandes de migration de machines virtuelles depuis l'appliance virtuelle AWS Connector. (Notez que le AWS connecteur utilise la politique gérée « AWSConnector » pour envoyer des demandes au nom du client au Import/Export service de machine virtuelle.) Permet de créer des AMI et des instantanés EBS, de modifier les attributs des instantanés EBS, d'effectuer des appels « Describe* » sur des objets EC2 et de lire à partir de compartiments S3 en commençant par « importer vers ec2 ».

VMImportExportRoleForAWSConnector est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer VMImportExportRoleForAWSConnector à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : Politique relative aux rôles de service
- Heure de création : 03 septembre 2015, 20:48 UTC
- Heure modifiée : 03 septembre 2015, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

VPCLatticeFullAccess

Description : fournit un accès complet à Amazon VPC Lattice et aux services de dépendance.

VPCLatticeFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer VPCLatticeFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 mars 2023, 02:49 UTC
- Heure modifiée : 12 février 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeFullAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
    }
  ]
}

```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

VPCLatticeReadOnlyAccess

Description : fournit un accès en lecture seule à Amazon VPC Lattice via le Console de gestion AWS, et un accès limité aux services de dépendance.

VPCLatticeReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer VPCLatticeReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 mars 2023, 02:47 UTC
- Heure modifiée : 12 février 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

VPCLatticeServicesInvokeAccess

Description : permet d'appeler les services Amazon VPC Lattice.

VPCLatticeServicesInvokeAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer VPCLatticeServicesInvokeAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 30 mars 2023, 02:45 UTC
- Heure modifiée : 30 mars 2023, 02:45 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique JSON

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


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

WAFLoggingServiceRolePolicy

Description : Création d'un réflex pour écrire les journaux des clients dans un flux Firehose

WAFLoggingServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 24 août 2018, 21:05 UTC
- Heure modifiée : 20 mai 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      }
    }
  }
]
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

WAFFirehoseLoggingServiceRolePolicy

Description : Création d'un rôle pour écrire les journaux des clients dans un flux Firehose

WAFFirehoseLoggingServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 24 août 2018, 18:40 UTC
- Heure modifiée : 20 mai 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
  }
}
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

WAFV2LoggingServiceRolePolicy

Description : Cette politique crée un rôle lié à un service qui permet à AWS WAF d'écrire des journaux dans Amazon Kinesis Data Firehose.

WAFV2LoggingServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Cette politique est associée à un rôle lié à un service qui permet au service d'effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

Détails de la politique

- Type : politique de Service-linked rôle
- Heure de création : 07 novembre 2019, 00:40 UTC
- Heure modifiée : 20 mai 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy`

Version de la politique

Version de la politique : v4 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
        }
      }
    }
  ]
}
```

```
}  
]  
}
```

En savoir plus

- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

WellArchitectedAgentResourceScanning

Description : accorde à l' AWS Well-Architected agent un accès en lecture seule aux configurations AWS des ressources, aux paramètres de sécurité et aux données opérationnelles afin de générer des recommandations d'optimisation

WellArchitectedAgentResourceScanning est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer WellArchitectedAgentResourceScanning à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 16 juillet 2026, 20:27 UTC
- Heure modifiée : 30 septembre 2026, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedAgentResourceScanning`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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",
"datzone:GetDataSource",
"datzone:GetDomain",
"datzone:GetDomainUnit",
"datzone:GetEnvironment",
"datzone:GetEnvironmentAction",
"datzone:GetEnvironmentBlueprintConfiguration",
"datzone:GetEnvironmentProfile",
"datzone:GetGroupProfile",
"datzone:GetProject",
"datzone:GetProjectProfile",
"datzone:GetSubscriptionTarget",
"datzone:GetUserProfile",
"datzone:ListConnections",
"datzone:ListDataSources",
"datzone:ListDomains",
"datzone:ListDomainUnitsForParent",
"datzone:ListEntityOwners",
"datzone: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",
"qlldb:DescribeJournalKinesisStream",
"qlldb:ListJournalKinesisStreamsForLedger",
"qlldb: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" : "*"
}
]
}

```


En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

WellArchitectedConsoleFullAccess

Description : Fournit un accès complet à AWS Well-Architected l'outil via le Console de gestion AWS

WellArchitectedConsoleFullAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer WellArchitectedConsoleFullAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2018, 18:19 UTC
- Heure modifiée : 09 juillet 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess`

Version de la politique

Version de la politique : v2 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique.

Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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"
      ]
    }
  }
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

WellArchitectedConsoleReadOnlyAccess

Description : Fournit un accès en lecture seule à l' AWS Well-Architected outil via Console de gestion AWS

WellArchitectedConsoleReadOnlyAccess est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer WellArchitectedConsoleReadOnlyAccess à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 29 novembre 2018, 18:21 UTC

- Heure modifiée : 09 juillet 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess`

Version de la politique

Version de la politique : v3 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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" : "*"
    }
  ]
}
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)

- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

WorkLinkServiceRolePolicy

Description : Permet d'accéder aux ressources utilisées ou gérées par Amazon Services AWS et de les utiliser WorkLink

WorkLinkServiceRolePolicy est une politique [AWS gérée](#).

Utilisation de cette politique

Vous pouvez associer WorkLinkServiceRolePolicy à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 23 janvier 2019, 19:03 UTC
- Heure modifiée : 23 janvier 2019, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy`

Version de la politique

Version de la politique : v1 (par défaut)

La version par défaut de la politique est la version qui définit les autorisations pour la politique. Lorsqu'un utilisateur ou un rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il faut autoriser la demande.

Document de politique 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-*"
  }
]
```

En savoir plus

- [Création d'un ensemble d'autorisations à l'aide de politiques AWS gérées dans IAM Identity Center](#)
- [Ajouter et supprimer des autorisations d'identité IAM](#)
- [Comprendre la gestion des versions pour les politiques IAM](#)
- [Commencez avec les politiques AWS gérées et passez aux autorisations avec le moindre privilège](#)

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.